Edited by:
Jane Duncan and
Allen Munoriyarwa

DEMOCRATISING SPY WATCHING

Public oversight of intelligence-driven surveillance in Southern Africa

SCOTTISH
UNIVERSITIES
PRESS

DEMOCRATISING SPY WATCHING

DEMOCRATISING SPY WATCHING

Public oversight of intelligence-driven surveillance in Southern Africa

Edited by
Jane Duncan and Allen Munoriyarwa

SCOTTISH
UNIVERSITIES
PRESS

First published in 2026 by
Scottish Universities Press
SUP Publishing CIC
International House
38 Thistle Street
Edinburgh
EH2 1EN

https://www.sup.ac.uk

ISBN (Hardback): 978-1-917341-13-4
ISBN (Paperback): 978-1-917341-12-7
ISBN (PDF): 978-1-917341-15-8
ISBN (EPUB): 978-1-917341-14-1
DOI: https://doi.org/10.62637/sup.dasw4926

All external links included were live at the time of publication.

An electronic edition can be downloaded free of charge at
https://doi.org/10.62637/sup.dasw4926
or scan the following QR code:

This book has been through a rigorous peer review process to ensure that it meets the highest academic standards. A copy of the full SUP Peer Review Policy & Procedure can be found here: https://www.sup.ac.uk/peer-review
Typeset by: Palimpsest Book Production Limited, Falkirk, Stirlingshire
Cover design: Nicky Borowiec
Front cover images:
Shadow figures: AdobeStock/Curto.
Camera: AdobeStock/Pixelly.

TABLE OF CONTENTS

LIST OF FIGURES

AUTHOR BIOGRAPHIES

Tachilisa Badala Balule is an Associate Professor of Law in the Department of Law, University of Botswana. He is currently the Deputy Dean in the Faculty of Social Sciences. He holds an LLB degree from the University of Botswana, and LLM and PhD degrees from the University of Edinburgh, Scotland. His PhD research was on regulation of the media. Dr Balule has published in the area of freedom of expression, including media freedom and access to information, and on aspects of electoral laws. He has delivered papers on freedom of expression, media law and access to information at national and international conferences. He has also written on digital surveillance, data protection and privacy in Botswana, and has completed a study recently on this topic. His research on digital surveillance was cited by both sides of the house in a parliamentary debate on the Criminal Procedure and Evidence (Controlled Investigations) Bill, that led to the Government of Botswana making significant concessions to the Bill's critics.

Sarah Chiumbu is an Associate Professor of Communication at the University of Johannesburg (UJ), South Africa. Prior to this, she served as a Senior Research Specialist in the Human and Social Development Research Programme at the Human Sciences Research Council (HSRC). She also spent seven years at the University of the Witwatersrand as a senior lecturer in Media and Communication Studies. She holds a PhD and MA in media studies from the University of Oslo, Norway. Her research interests encompass media, democracy and citizenship, digital media, policy studies and social movements.

Jane Duncan is a Professor of Digital Society at the University of Glasgow and she holds a British Academy Global Professorship at the same university. The Professorship supports comparative case-study research on strengthening public oversight of intelligence-driven surveillance in eight Southern African countries. She is also a Visiting Professor at the University of Johannesburg. Before that, she was a Professor in the Department of Communication and Media at UJ from 2014 to 2022. Between 2018 and 2020, she was Head of Department of Journalism, Film and Television at UJ. In 2018, she was appointed by President Cyril Ramaphosa to a panel to investigate abuses of the State Security Agency (SSA). Before joining UJ, she held the Chair in Media and Information Society in the School of Journalism and Media Studies at the University Currently Known as Rhodes. She comes from a civil society background, having worked for the South African-based Freedom of Expression Institute (FXI) for 15 years and having served as its Executive Director for eight of those years. She has produced five single-authored peer-reviewed books and is a regular contributor to a range of journalistic publications.

Frederico Links is a Namibian governance researcher and a journalist focusing on state-related governance issues. He has coordinated and contributed to projects at national, regional and international levels. He is the lead researcher for Namibia in the eight-country digital-surveillance research project funded by the British Academy, through the University of Glasgow. He also recently contributed to a study on cybersecurity and cybercrime laws and their impacts on media freedom and free expression across the Southern African Development Community (SADC) region. Aside from his journalism and research work, Links is also the founding and current chairperson of the Access to Information in Namibia (ACTION) Coalition of civil society and media organisations and social activists. The ACTION Coalition has been instrumental in successfully advocating for an access to information law in Namibia since 2012. Links is the author of a large number of articles, reports and book chapters.

Rafael Marques de Morais serves as the executive director of the Centro de Estudos Ufolo para a Boa Governação (Ufolo Center for Good Governance), and he is the founder of Maka Angola, the country's leading anti-corruption watchdog.

Trésor Maheshe Musole is a professor of international law at the Catholic University of Bukavu, in the east of the Democratic Republic of Congo (DRC). He specialises in issues of peace, human rights, security and migration in the Great Lakes region, as well as freedom of expression and the right to asylum. As such, he is a member of the Law and Migration Team at the Catholic University of Louvain, where he teaches as a visiting professor. He has experience in the legal and human rights fields, having worked as a barrister in South Kivu in the DRC. He recently completed a study on digital surveillance and privacy in the DRC: balancing national security and personal data protection.

Allen Munoriyarwa is an Associate Professor of Journalism at Walter Sisulu University (WSU) in South Africa, in the Department of Marketing, Public Relations and Communication. His research interests include surveillance and cultures of digital media and journalism. He has published widely in these areas and is the former coordinator of the Media Policy and Democracy Project (MPDP), a research project that explored the growth of digital surveillance practices in Southern Africa. He is also a board member of Intelwatch, a civil society organisation that operates internationally.

Ernesto Nhanale is both an academic and a civil society activist, having served as the director of the Mozambique chapter of the Media Institute for Southern Africa for several years. He is also a Professor of Media and Journalism at Higher School of Journalism, an independent higher-education institution in Mozambique. He has undertaken extensive research work and produced publications in the area of political communication and journalism and is a co-founder of CEC – Centre of Interdisciplinary Studies of Communication. He recently completed a study on digital surveillance and authoritarianism in Mozambique.

Borges Nhamirre is a researcher on peace, security and governance at the Institute for Security Studies (ISS Africa). Prior to joining ISS in 2021, he served as a senior researcher and research coordinator at the Centre for Public Integrity in Maputo. He holds a Master's degree in Security Studies with a specialisation in Maritime Security from Joaquim Chissano University in Maputo, and he is currently pursuing a PhD in History of Ethnicity and Conflict in Northern Mozambique at Queen's University Belfast (QUB), Northern Ireland. He also lectures on Nationalism and Liberation Movements in 20th-century Africa at the School of History, Anthropology, Philosophy and Politics at QUB.

Phillip Santos teaches both undergraduate and postgraduate courses in the Department of Journalism and Media Technology at the Namibia University of Science and Technology and is Research Associate in the Department of Strategic Communication, University of Johannesburg. He also taught in the Department of Journalism and Media Studies at the National University of Science and Technology in Zimbabwe. He holds a PhD from Rhodes University in South Africa and co-edited the books *Reading Justice Claims on Social Media: Perspectives from the Global South* and *Global Pandemics in the Media: An African Perspective*. His research interests are in political and strategic communication; the mediation of science and health issues, social memory, gender, justice and political struggle; the social and policy dimensions of new and broadcast media, as well as the confluence between political correctness, populism, post-truthism and democratic politics.

Rui Verde holds a PhD in Law from the University of Newcastle, UK, and a law degree from Universidade Católica de Lisboa, Portugal. He serves as Chief Legal Adviser to Maka Angola, an organisation committed to promoting democracy, defending human rights and combating corruption in Angola. An expert on Angola's legal landscape – especially in matters concerning corruption, the exercise and integrity of judicial authority, the dynamics of contemporary politics, and the evolving landscape of surveillance and digital rights – he has published extensively on these topics. At Oxford University, he developed a research project examining China's influence in Angola and has completed a study on the role of the Israeli surveillance industry in the country. Currently a Research Associate at the African Studies Centre, University of Oxford, and Chercheur Associé at CEPED, Université Paris-Cité, he also founded the think-tank CEDESA, which is dedicated to advancing development in Southern Africa.

LIST OF ABBREVIATIONS

ADF	Africa Defence Forum
ANC	African National Congress (South Africa)
ANR	Agence Nationale de Renseignements (DRC)
ARPTC	Autorité de Régulation des Postes et Télécommunications (DRC)
BDF	Botswana Defence Force
BOCONGO	Botswana Council of Non-governmental Organisations
BOSS	Bureau of State Security (South Africa)
BPS	Botswana Police Service
CAT	Campaign Action Teams
CCTV	Closed-circuit television
CDD	Centre for Democracy and Human Rights (Mozambique)
CIA	Central Intelligence Agency (United States)
CIC	Central Intelligence Committee (Botswana)
CICC	Controlled Investigations Coordinating Committee (Botswana)
CIO	Central Intelligence Organisation (Rhodesia/Zimbabwe)
CIP	Center for Public Integrity (Mozambique)
CLC	Comité laïc de coordination (DRC)
CRAN	Communications Regulatory Authority of Namibia
CRONGD	Conseil régional des organisations non gouvernementales de développement (DRC)
CSO	Civil Society Organisation
DCAF	Geneva Centre for Security Sector Governance

DCEC	Directorate on Corruption and Economic Crime (Botswana)
DFID	Department for International Development (United Kingdom)
DG	Director General
DIS	Directorate of Intelligence and Security (Botswana)
DISA	Directorate of Information and Security of Angola
DPA	Data Protection Authority (DRC)
DPA	Data Protection Act (Mauritius)
DRC	Democratic Republic of the Congo
FCDO	Foreign, Commonwealth and Development Office (United Kingdom)
FNLA	Frente Nacional de Libertação de Angola (National Front for the Liberation of Angola)
FRELIMO	Frente de Libertação de Moçambique (Mozambican Liberation Front)
FTAF	Financial Action Task Force
GPS	Global Positioning System
HRC	United Nations Human Rights Committee
HTTPS	Hypertext Transfer Protocol Secure
ICA	Information and Communication Act (Zimbabwe)
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technologies
ID	Identity
IDT	Information for Development Trust (Zimbabwe)
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
INACOM	Instituto Angolano das Comunicações (Angolan Institute for Communications)
INCM	Instituto Nacional das Comunicações de Moçambique (Mozambican National Institute of Telecommunication)
IP	Internet Protocol
IPPR	Institute for Public Policy Research (Namibia)
ISS Act	Intelligence and Security Service Act
JSCI	Joint Standing Committee on Intelligence (South Africa)

LAC	Legal Assistance Centre (Namibia)
MICT	Ministry of Information and Communication Technology (Namibia)
MISA	Media Institute of Southern Africa
MLP	Mauritian Labour Party
MMM	Mouvement Militant Mauricien (Mauritius)
MNA	Member of the National Assembly (Zimbabwe)
MNIS	Mauritius National Identity Scheme
MPDP	Media Policy and Democracy Project
MPF	Mauritian Police Force
MPLA	Popular Movement for the Liberation of Angola
MSCP	Mauritian Safe City Project
MSF	Multiple Streams Framework
MSM	Mouvement Socialist Militant (Militant Socialist Movement) (Mauritius)
NA	National Assembly
NCG	National Coast Guard (Mauritius)
NCIS	Namibia Central Intelligence Service
NGO	Non-governmental organization
NIC	National Identity Card (Mauritius)
NMT	Namibia Media Trust
NPF	National Police Force (Mauritius)
NSA	National Security Agency (United States)
NSC	National Security Council (Zimbabwe)
NWG	National Working Group (South Africa)
PCIS	Parliamentary Committee on Intelligence and Security (Botswana)
PIDE	Polícia Internacional e de Defesa do Estado (Portuguese Secret Police)
PISI	Police Internal Security and Intelligence (Zimbabwe)
PMSD	Parti Mauricien Social Démocrate (Mauritian Social Democratic Party)
PPI	Partnership for Integrated Protection (DRC)
R2K	Right2Know Campaign (South Africa)
RAM	Register of Mobile Appliances (DRC)
RENAMO	Mozambican National Resistance
RF	Rhodesian Front

RFI	Radio France International
RHADOSKI	Réseau des associations des droits de l'homme du Sud-Kivu (DRC)
RSF	Reporters sans frontières (Reporters Without Borders)
SADC	Southern African Development Community
SAM	Secure Access Module
SAPS	South African Police Service
SCCIA	Informação dos Serviços de Centralização e Coordenação da Informação de Angola (Angolan Centralisation and Coordination of Information Services)
SIE	External Intelligence Service (Angola)
SIM	Subscriber Identity Module
SINSE	Serviço de Inteligência e Segurança de Estado (State Intelligence and Security Service) (Angola)
SISE	Serviço de Informação e Segurança do Estado (State Intelligence and Security Service) (Mozambique)
SISM	Serviço de Inteligência e Segurança Militar (Military Intelligence Service) (Angola)
SMF	Special Mobile Force (Mauritius)
SNASP	Serviço Nacional de Segurança Popular (National Security and Public Order Service) (Mozambique)
SSA	State Security Agency
SWAPO	South-West Africa People's Organization
UK	United Kingdom
UN	United Nations
UNITA	União Nacional para a Independência Total de Angola (National Union for the Total Independence of Angola)
US	United States
VP	Vice Presidency (Zimbabwe)
ZANLA	Zimbabwe African National Liberation Army
ZANU-PF	Zimbabwe African National Union – Patriotic Front
ZAPU	Zimbabwe African People's Union
ZDF	Zimbabwe Defence Forces
ZIPRA	Zimbabwe People's Revolutionary Army
ZRP	Zimbabwe Republic Police

FOREWORD

In several countries discussed in this book, invoking state security has become synonymous with hostility towards freedom of expression and the press. This leads to fear, oppression, abuse of power and, ultimately, the capture of state institutions.

Why does this happen? Experts featured in this volume provide insightful answers. At its core, it is arguably about disempowering citizens by restricting access to information – an essential tool for providing oversight of state institutions. Such oversight ensures these institutions serve the common good, strengthens their capacity and upholds accountability.

I share a glimpse of my personal journey as someone targeted by state security and private contractors serving the powerful, with the help of foreign interests seeking business advantages. My experience highlights the grim reality faced by individuals who stand up for justice and the steep price they often pay. As an investigative journalist and self-described troublemaker, I dared to expose and challenge those who plundered Angola, further impoverishing its majority and robbing citizens of their future. For years, many Angolans and foreign nationals asked me the same question: How are you still alive? The sheer necessity of that question is a chilling reminder of the dangers that accompany resistance to misrule.

One incident vividly illustrates the reach of the state security apparatus. For several years, a relative persistently asked to visit me and introduce me to his daughter, whom he had named after me. I had resisted to protect him from any potential consequences due to his background in state security. Eventually, I agreed. When he entered my living room, he was visibly shocked, shaking and sweating profusely. Upon arriving at the square where I lived, he had crossed paths with a colleague who informed him that he had been assigned to surveil 'the journalist', and that a command post had been established in the square for that purpose. I was the journalist in question.

Next door to my residence, in a house rented by an investment firm, an Israeli-led company had installed a stationary surveillance van equipped with advanced digital monitoring equipment. Its wheels had been removed to keep it in place, enabling 24/7 surveillance of my home. In 2013, security researcher Jacob Appelbaum discovered custom-designed malware on my laptop, covertly collecting all my information and sending it to India. He traced the malware to a Western multinational company based in Portugal that was providing IT security solutions and auditing services to the Angolan government. As reported in *Newsweek*, this company played a direct role in facilitating my surveillance.

Surveillance was only part of the campaign against me. Concurrent measures sought to isolate me completely and even included an attempt on my life abroad. A superior order reportedly cancelled the execution just five minutes before it was to occur.

For years I remained in denial, unable to fathom that my investigative work, published mainly on a modest website called Maka Angola, could make me an enemy of the state – or more accurately, of those who had captured the state. Gradually, I came to understand the extent of the threat my work posed to those in power, especially as I gained access to intelligence reports detailing the monitoring of civil society, including myself.

Interestingly, I also received indirect help from anonymous individuals within the state security apparatus. Some believed, as I did, that each person had a role to play in building a better Angola. Their quiet resistance to misrule enabled me to survive. This goodwill only underscored how dangerous my work was perceived to be by those in power.

In 2017, Angolans celebrated the end of 38 years of rule by José Eduardo dos Santos, with hopes that President João Lourenço would usher in a new era of reform. However, Lourenço continued the same system of governance without enacting fundamental reforms in the judiciary or state administration. He maintained the ruling Popular

Movement for the Liberation of Angola's (MPLA) modus operandi, which had entrenched state capture. By 2018, as MPLA leader, he further consolidated power, overseeing a government plagued by dysfunction, corruption, incompetence and plunder.

To shield this misrule, Lourenço expanded his repressive apparatus. By 2024 he effectively merged the Ministry of Interior with the Directorate of Intelligence and State Security Service (SINSE), circumventing legal frameworks meant to separate their functions. Senior intelligence officers were appointed to lead the Ministry and its critical departments like the Criminal Investigation Service. With SINSE accountable only to the President, Angola's state-security apparatus was transformed into a tool for maintaining power rather than protecting the public.

This misuse of state security reflects broader patterns in authoritarian regimes, where such systems are weaponised to suppress dissent and protect corruption. These actions undermine governance, erode public trust and disempower citizens. When these institutions serve oppressive regimes, they betray their fundamental purpose, enabling misrule and depriving citizens of the freedoms necessary to secure their future.

State-security agencies in the eight countries under study in this book must be reminded of their true mission: to protect the citizens.

Legal frameworks and formal protocols for oversight often fail because they depend on the very institutions they are meant to regulate. The most effective oversight stems from public scrutiny, enabled by a free press, academia, activists and civil society. By amplifying public awareness and pressuring for transparency, these entities are vital to holding state security accountable and ensuring governance serves the common good.

Rafael Marques de Morais

ACKNOWLEDGEMENTS

We would like to acknowledge the support of the British Academy's Global Professorship programme (grant number GP/400069), which made the research included in this edited volume possible, and we thank them for this support. We also acknowledge and thank the College of Social Sciences and School of Social and Political Sciences, University of Glasgow, for hosting the research; particularly the Division for Sociological and Cultural Studies. We are grateful to the Department of Communication and Media in the Faculty of Humanities at the University of Johannesburg for also continuing to show support for the project, and one of the editors continues to hold a formal affiliation with the Department. We are also grateful to WSU for giving co-editor Allen Munoriyarwa valuable time away to conclude this research project. Lastly, we acknowledge all those who participated in this project and thank them for their time and commitment.

Jane Duncan and Allen Munoriyarwa

CHAPTER ONE

Making the case for public oversight of intelligence-driven surveillance: Key issues and core concepts

Jane Duncan and Allen Munoriyarwa

Introduction

Technological developments, government obsessions with secrets and legal vacuums across different countries have conspired to give the intelligence communities unprecedented insights into people's private lives and power over their private conduct (Granick, 2017). Digital surveillance has been used to hinder or monitor groups and individuals that seek to change the political, economic and social conditions of their communities. For example, in 2022, Botswana's intelligence agencies attempted a major power grab. They sought wide-ranging powers through a draft law that would allow them to intercept communications on a warrantless basis, including the communications of journalists. These powers would have weakened basic democratic controls over surveillance for intelligence purposes, especially judicial controls over surveillance through prior authorisation. However, their power grab was thwarted by the public (Ndlovu, 2022). The media, civil society and trade unions objected to the draft law, the Criminal Procedure and Evidence (Controlled Investigations) Bill, but dubbed the 'Spy Bill' by its critics. The ensuing controversy was so huge and impactful that it forced the government to walk back draconian provisions in the Bill, although the law that was passed eventually was far from perfect (Balule and Dambe, 2023, pp. 1–14).

Botswana provides a very recent example of a poorly understood but, at times, highly effective form of oversight of intelligence-driven surveillance, namely public oversight. Similar surveillance scandals have erupted across Southern Africa, where publics have exposed and reacted to surveillance by intelligence agencies, when it has been used for improper and even unlawful purposes. In an earlier case in Angola, in 2015, and in what has become known as the 15+2 or Luanda reading-club case, 17 activists were charged with preparatory acts of rebellion, and plotting against the president and other state institutions. Their crime? Holding a reading group on non-violent resistance, which included a translated version of a Gene Sharp book, entitled *Tools to Destroy a Dictator*. Angolan intelligence officers used covert digital video surveillance to monitor the reading group, and the recordings were then used in the trial. Concerned citizens groups launched a major international solidarity campaign, leading to the Supreme Court granting their conditional release followed by an amnesty law that was applied to them (Verde, 2021, pp. 7–9). In South Africa, and over a decade starting in 2011, a major multi-class campaign led by civil society and social movements prevented two successive presidents from signing a Bill into law that would have drawn a shroud of secrecy over the police and intelligence agencies (the 'Secrecy Bill'), and an investigative journalism non-profit organization, the amaBhungane Centre for Investigative Journalism, successfully challenged the country's main law (under) regulating digital surveillance. In Mauritius, from 2013 onwards, a public push-back against the surveillance potential of a government smart identity card led to the government having to abandon its ambitions to establish a centralised biometric database of all personal citizen data (Duncan, 2022, pp. 121–2).

As the chapters in this book will show, these scandals have followed familiar patterns across time and space. Intelligence agencies are meant to use surveillance capabilities for pressing public purposes, such as protecting national security and solving serious crimes when they have exhausted other, less intrusive, investigative methods. However, the notoriously secretive work of intelligence creates the potential for abuse, especially in circumstances where intelligence agencies focusing on national security are poorly controlled and overseen, and digitisation has compounded these problems (Gill and Phythian, 2012, pp. 92–3; Munoriyarwa and Mare, 2023, pp. 6–8). Governing parties concerned about maintaining their grip on the levers of power may well be tempted to use (and as this book will show, have used) these capabilities to put perceived and actual critics under surveillance to provide them with the upper hand. Yet, time and again, the law and oversight practices have not kept up with intelligence agencies' technological capabilities to surveil. It is more likely that details about law-enforcement surveillance will come into the public domain, given its focus on collecting intelligence for prosecutorial purposes, and hence police surveillance practices are more likely to be scrutinised in court. National security intelligence, on the other hand, and the surveillance practices used to collect it, is often more wide-ranging and even speculative, as it is focused on broader, longer-term threats to a country (strategic intelligence) and measures to counter them (counter-intelligence). As it is generally not prosecutions-focused, this form of intelligence, and the surveillance used to collect it, may be even more open to abuse than police intelligence. However, increasingly, there is a blurring of the lines between law-enforcement intelligence and national-security intelligence, with secretive practices from the latter being transported into the former, which can heighten the potential for abuse of the former.

Consequently, when it occurs, surveillance overreach may come into the public domain only through public exposures, leading to surveillance controversies and even scandals and, in countries where organisational capacity exists to take these issues up, activism to rein these powers in. Some of these scandals have led to major democratic victories, where organised public responses have forced intelligence agencies to become more transparent in how they use these capabilities on a long-term basis. Other controversies have led to mixed outcomes and still others have failed to achieve any meaningful concessions. This book examines the lessons to be learnt from key moments when publics have attempted such oversight in eight Southern African countries (Angola, Botswana, Democratic Republic of the Congo, Namibia, Mauritius, Mozambique, South Africa and Zimbabwe). These countries were chosen because they span the spectrums of equality and democracy in Southern Africa, and the major linguistic divides in the region. They also have different, but still ever-present, colonial histories that continue to shape how their intelligence and security sectors operate, making them ripe for comparison.

This introductory chapter deals with the main objectives and key questions of the research project that informs this edited volume, the methodology used, some of the core concepts engaged in this book and how they are understood. It also introduces the chapters in the book. The chapter also sets the basis for the analyses that follow on the practices of the media and civil society organisations as a neglected but much needed dimension of oversight (Kniep et al., 2023, p. 7).

Objectives and key question

Governments justify digital surveillance as being necessary to fight crime and terrorism: social ills that could undermine attempts to ensure that citizens enjoy substantive freedoms and real opportunities. Consequently, digital surveillance is becoming increasingly popular in policing and intelligence work in Southern Africa, where data protection rules and intelligence oversight are generally weak. Such surveillance involves unique risks to privacy, in that it enables automated tracking of individuals across widening geographical distances on a continuous, real-time basis, which has tilted corporate and state modes of surveillance increasingly towards everyday life (Lyon, 2018, p. 12). Since the September 11, 2001 terrorist attacks on the United States (US), intelligence agencies and private sector companies have developed an elective affinity (Zuboff, 2019, p. 116). The agencies had a vested interest in collecting as much data as possible, ostensibly to prevent further intelligence failures on the scale of the one that allowed the September 11 attacks to happen, while private companies, such as Google, had a vested interest in preventing restrictions on their business models on privacy grounds. This convergence of interests led to unprecedented collaborations between intelligence agencies and Silicon Valley firms, and to conditions for what Shoshana refers to, with reference to Giorgio Agamben's states of exception, as surveillance exceptionalism (Zuboff, 2019, p. 116), or a situation where secret public–private intelligence collaborations are stitched together that greatly expand intelligence powers while making oversight even more difficult than it was.

The available evidence points to Southern African societies facing a major – and under-analysed – surveillance problem, where the technological capabilities of intelligence agencies have run far ahead of the capabilities of the judiciary, administrative and legislative bodies, to perform effective oversight, and where there is limited evidence of these capabilities being used for legitimate public purposes. The chapters will include contextual information where this state of exception following the September 11 attacks played out in Southern Africa, which, despite being somewhat removed from the immediate aftermath of 9/11, saw some governments seizing on the war on terror to expand surveillance powers, and enlisting the private sector or other governments to assist with their compliance with the requirements of bodies such as the Financial Action Task Force to combat terrorism financing. Other governments were galvanised mainly by domestic factors – such as rising protest action – to expand their capabilities by buying surveillance technologies from an increasingly globalised and privatised industry.

The background to this book is that one of the editors, Jane Duncan, was awarded a British Academy Global Professorship, lasting four years and starting in January 2023, and she set up a research project to explore public oversight practices in eight Southern African countries, using a comparative case-study methodology. The contents reflect on the findings of the first two years of the project. It assesses the adequacy of oversight in the eight countries, based on the conviction that the mere establishment of formal oversight institutions is unlikely to deliver substantive accountability, where intelligence contributes in meaningful ways to ensuring the kinds of radical justice and equality that have evaded these countries, despite liberation from colonialism and apartheid. This is not to say that there should not be aspirations to establish such institutions, particularly in semi-authoritarian countries, where their establishment could be a galvanising force in society. However, truly effective oversight and, ultimately, accountability will most likely have reach beyond these institutions and incorporate a mobilised public, as there is little sense in prescribing the same remedies to digital surveillance overreach that have been implemented elsewhere, but with unsatisfactory results. Therefore, this book takes these weaknesses into account and uses them to analyse moments when public oversight has been attempted as a supplement to, and even a replacement for, more conventional forms of oversight, and lessons to be learnt from them.

A challenge the authors faced was that intelligence is notoriously difficult to study, as primary sources of information, including interviews, may be limited by secrecy (van Puyvelde, 2018, pp. 375–91). These limitations apply especially to national security intelligence, where countries typically tend to tolerate executive discretion in using surveillance, coupled with higher levels of secrecy, when compared to other areas of government, and this problem is compounded in countries with serious democracy deficits. In view of these difficulties, researchers may be tempted, understandably, to focus on structural accounts of intelligence systems, including oversight, by using publicly available sources such as laws and policies. Assessments of their democratic or authoritarian content may be made depending on the presence or absence of legislative or policy checks and balances, summarised in international standards (Wegge and Wentzling, 2018, pp. 26–8). We, on the other hand, have chosen to adopt an agential approach to oversight: in other words, while documenting the dangers of surveillance overreach, we also proceed from the assumption that intelligence systems are not static and that, in certain conditions, publics can and do have causal power in shaping and reshaping these systems. We are interested in those forms of agency that increase the accountability of these most secretive areas of government and allow publics to exercise informed digital citizenship and challenge state and private surveillance power (Hintz et al., 2019, pp. 123–43; Choudry, 2018, pp. 3–22). We intended the research to be forward-looking, addressing the question of what kinds of agency are possible, even in the most difficult of contexts.

Crucially to the authors, the risks of intelligence abuses, and of digital technologies being used in ways that mainly benefit dominant elite interests, are tightly connected to public acceptance or rejection of levels of surveillance (Duncan, 2018, pp. 185–204; Hintz et al., 2019, pp. 117–21), which in turn impacts on whether sections of the public are open to being galvanised on this issue. As data-mining practices increase, publics risk becoming resigned to living without any reasonable expectation of privacy, and with no expectation of being able to associate and organise freely and without state intervention. Where there is little or no expectation of privacy, such societies risk being subjected to near-ubiquitous uses of dragnet digital surveillance, where huge quantities of data are collected and analysed, irrespective of whether there is a reasonable suspicion of criminality. Intelligence abuses thrive in societies that are not informed about surveillance and that are resigned to the perceived 'realities' of security overreach and surveillance realism (Dencik, 2018, pp. 31–43). Therefore, understanding the role of public perceptions and the circumstances in which these perceptions translate into opposition and, ultimately, action directed towards strengthening oversight of intelligence on a more sustained basis (especially in contexts where strong official oversight is lacking) is crucial to understanding how we limit a potential spiral of surveillance overreach.

This agential approach, and its possibilities and limits, is particularly relevant in a peripheral region of the world like Southern Africa, whose insertion into the global economy has been shaped fundamentally by colonialism, imperialism and, more recently, apartheid. Popular struggles against these forms of repression and exploitation led to substantial democratic gains, but subsequent transitions to independence and democracy failed to provide a genuine incorporation of the masses into the resulting political systems (Saul, 2005, pp. 17–31). Consequently, post-apartheid and postcolonial government efforts to transform intelligence systems from being tools of repressive rule to ones that were more representative of the publics they were meant to serve and protect, were incomplete and subject to democratic reversals (Duncan, 2022, p. 37–68).

Where public oversight has been studied, attention has been confined mainly to the Anglosphere and the global north, where there is a long and rich history of public oversight (see, for example, the role of journalists and public-interest groups in relation to Church Committee on intelligence abuses in the US; van Puyvelde, 2012, pp. 139–58), particularly in the wake of the whistleblowing on surveillance abuses by Wikileaks founder Julian Assange and former National Security Agency (NSA) contractor Edward Snowden (Shiraz and Aldrich, 2019, pp. 1,313–29). While their claims to the status of whistleblowers have been contested, as their disclosures of classified information went beyond what would be considered acceptable whistleblower conduct (see, for example, US House of Representatives (2016)), there can be little argument that their main motivations were to expose government wrongdoings, which is what they did, and there can also be little argument that the formal oversight structures failed to correct the wrongdoings. This book attempts to correct these biases, and to focus attention on what can be learnt from the postcolonial, post-apartheid contexts across Southern Africa, with unstable political systems that range from the superficially democratic to the semi-authoritarian. Contrary to what may be assumed at the outset, it is very possible to research intelligence and its oversight in such systems, precisely because of their relative instability.

The question is, how best can we make intelligence serve the public interest: that is, focus only on real threats (Granick, 2017) to national security and public safety? Public mobilisation can lead to successful court cases to limit surveillance powers, as was the case in South Africa, or those with technological know-how can use defensive technologies to shield themselves from surveillance (Granick, 2017). However, not all publics have access to independent judiciaries or the technological means to defend themselves, which raises the question: in circumstances where there may be limited options of litigation, and if anti-surveillance technologies are expensive, where do we go from here? The answer is to the public. However, this response triggers further questions. For example, how should publics constitute themselves to hold intelligence agencies to account for how they use digital surveillance? Are there any specific practices that public oversight should focus on and what are their strengths and weaknesses? Thus, the main research questions could be distilled as follows:

- What are the examples for successful public oversight, what accounts for the successes and what are the indicators of success? To what extent are these successes sustainable in the context in which they happened?
- What are the examples of failed public oversight and what accounts for the failures?
- What are the examples of attempts at public oversight with mixed outcomes and why did they fail to achieve complete success or complete failure?
- To what extent could the successes be replicated elsewhere across time and space and the failures or unclear outcomes avoided? What are the elements that would go into the development of a set of theoretical propositions that could be applied and guide public oversight elsewhere?

Methodology

The authors of these chapters were contracted under the global professorship to conduct the in-country research. To that end, they established research teams based in each Southern African country, and collected data through key informant interviews, focus-group discussions with key activists, document and policy analysis, and content analysis of media and news content. They identified case studies consisting of events that triggered public controversies or scandals about possible surveillance overreach. These events included moments when draft legislation or policies on surveillance, or initiatives with surveillant potential (for example, smart Identity (ID) card or Subscriber Identity Module (SIM) card registration systems) were introduced, or when information about unjustifiable surveillance of politicians, activists or journalists erupted into the public domain. They examined public responses to these moments and the factors that influenced the extent to which the public challenges to unaccountable surveillance were successful or not. The authors sought out actors from key constituencies that were central to these moments, including parliamentarians and members of government, the private sector, lawyers, the media, non-governmental organisations (NGOs) and social movements, and approached them for interviews. They sought ethical clearance in all eight countries, as well as the United Kingdom (UK), and the process of doing so was fraught with complexity due to the sensitivity of the research, and the difficulties of identifying ethical clearance bodies that were independent from the state and the ruling party.

The key question the authors focused on was how could the public perform more effective oversight digital surveillance for intelligence purposes? This question drove them to examine the factors that strengthened and weakened attempts at effective public oversight, the forms of public oversight that were the most and least effective, how they were organised and to what end. They also examined how effective public oversight could be sustained over time.

The chapters of this book provide historical and contemporary evidence of intelligence surveillance violations that, therefore, make a case for a publicly driven oversight mechanism in which the public make periodic assessments and evaluation of both surveillance practice and technologies' purchase. The actors constituting these publics included more well-organised formations with or without significant social bases, such as NGOs, social and political movements, including trade unions and youth movements, the media, lawyers, public intellectuals and academics, as well as outpourings of public opinion that took less well-organised forms, such as responses to media articles, signatories to petitions, participants in protests and public debates and the like.

The research that informed this book used a comparative case study methodology, which allowed for large-scale contextual comparisons and for both depth and scope in analysis (Voltmer and Kraetzschmar, 2015; Esser, 2019, pp. 85–101). This combination enabled explorations of the eight countries, while allowing for higher-order generalisations about what works and what does not when it comes to public oversight and recognising that it is important not to overdetermine the ability of surveillance to discipline and punish dissent (Choudry, 2018, p. 7). The comparative elements were grouped into four major themes: historical legacies, institutional organisation of oversight, mobilisation of public oversight and dynamics of conflict escalation/settlement around intelligence oversight. The research followed a most similar systems design, as all country case studies are based in Southern African countries that have similar histories of colonialism, intelligence abuses and anti-colonial/anti-apartheid struggles, and contemporary surveillance practices that have not broken sufficiently from their apartheid/colonial pasts. The intention was to identify the differences or variables that account for successful public oversight of intelligence-driven surveillance: so why has such oversight been more successful in some countries than in others, despite these shared histories and geographic proximities?

While this book focuses mainly on the case studies, it makes reference to the above-mentioned comparative elements too, as they guided the data collection across the different countries. Each researcher pursued separate case studies of critical moments when public oversight had been attempted, but using an interview guide that contained cross-cutting, common question areas that enabled comparability of the case studies. The case studies were instrumental in that they were conducted to achieve a larger goal, which was to develop more general theories around possibilities for public oversight that apply across all cases and are of more general application (Micova, 2019, pp. 71–84).

The approach adopted was inductive, as the researchers developed the case studies and then compared them to explain conditions for successful public oversight, and qualitative, as the intention was not to prove a hypothesis, but to open possibilities for better oversight. However, there were assumptions that underpinned the research, which it would be fair to spell out at the outset. We proceeded from the assumption that public oversight of digital surveillance is a poorly acknowledged, but important and, at times, decisive factor in the success or failure of oversight and, intelligence accountability. We also suspected that, when there is surveillance overreach, then organised responses are more likely to be effective than individual responses. We had suspicions that divisions in the political elite and the presence of mass movements supported by

NGOs, coupled with weak social contracts, can increase the potential for effective public oversight, as elite consensus around the need for surveillance may be weaker. We decided to put our assumptions and suspicions to the test, while remaining open to new possibilities that we had not considered.

The authors' eclectic approaches and theoretical outlook

The chapters are written by researchers with backgrounds in communication and media studies and law, who draw on the insights offered by their various fields, as well as politics and sociology, civil society practitioners and journalists, and the chapters offer a mix of more descriptive and theoretical approaches. The authors have deep knowledge of these societies and were well placed to develop bottom-up solutions to oversight problems. They were acutely aware of the risks of undertaking this research but were convinced that the potential benefits far outweigh the risks and, in fact, that not undertaking the research posed the greater risk to these societies.

The authors adopted eclectic approaches to their case studies, which is fitting for a project traversing several disciplines. No attempt was made to force a theoretical outlook on the authors, with approaches ranging from radical democratic and Marxist to political process theory: however, overall, the volume aligns most closely with the critical paradigm. For example, researchers were concerned, not only with focusing on surveillance and its impacts on individual privacy, but with surveillance and its roles in maintaining unjust and unequal societies (see, for example, Fuchs, 2010, pp. 1–22; Bellamy Foster and McChesney, 2014; Yong Jin, 2015; Giroux, 2015, pp. 108–40; Hintz et al., 2019; Couldry and Meijas, 2019, pp. 336–49; Mann and Daly, 2018, pp. 379–95), which the countries being studied largely are, despite transitions from colonialism and apartheid. Focusing on surveillance in this way means that it becomes understood as one of several social-control mechanisms that need to be tackled if substantive emancipation is to be achieved. Its oversight then becomes understood as a practice that needs to extend beyond the assumptions of representative democracy, where official oversight bodies are touted as a panacea for intelligence abuses. The researchers were also motivated by a commitment to using their research to call the powerful to account – rather than engaging in administrative research that aims to solve practical problems without changing the power structures in which they operate – and in the process aimed to change how intelligence is organised to include a broader range of oversight actors as legitimate actors.

There is, however, a paucity of literature on intelligence and surveillance oversight from a critical perspective, perhaps due to the lack of critical distance between scholarship in intelligence studies and the intelligence institutions and practices being studied (Kniep et al., 2023, p. 3). The existing literature on these issues tends to be dominated by definitions of 'oversight' that are influenced by liberal democratic thinking, informed by consensual rather than conflictual views of democracy, and revolve largely around examinations of official institutional actors and practices, such as ministers, parliamentary committees and ombuds offices (Kniep et al., 2023, p. 2). In this world-view, the state is a politically neutral instrument of the will of the people, and state institutions that perform oversight of surveillance are understood as inherently technocratic institutions with the innate potential to serve the broader public good. Oversight institutions that stray from their ultimate objectives of ensuring intelligence, lawfulness and efficacy veer towards regulatory capture perspectives, where regulators (or, in this case, overseers) prioritise sectional interests over the broader public interest (see, for example, Pillar, 2010, pp. 423–78; Gill and Phythian, 2012, pp. 179–99). When that legitimacy is damaged by rogue spies, then reforms are intended to restore that legitimacy. However, the liberal account ignores the legacy of racism, class oppression and colonialism, where certain social groups attract intelligence interest by virtue of their already diminished position in society (Choudry, 2018, pp. 7–9). Such accounts cannot conceive of a situation where entire intelligence agencies can be discriminatory, abusive or unprofessional. A key theme of this edited volume is how postcolonial intelligence agencies have continued colonial-era surveillance practices of containing dissent, with little interruption in the social control purposes of intelligence despite independence.

Core concepts used in this book

It is necessary to set out how we understand some of the core concepts used in this book, as a number of them tend to suffer from the deficiency of weak conceptualisation. Our working definition of surveillance is a set of practices that involve the systematic, routinised collection and analysis of information and the accessing of personal data for the purposes of social control. This definition separates surveillance out from other forms of periodic monitoring or information collection and analysis for more routine everyday functions. There are dangers in defining surveillance too broadly, such as the systematic collection, storage and processing of information by a variety of actors in many fields of life and for a variety of purposes (see, for example, Lyon, 1994, pp. vii–x; Clark, 1988, pp. 498–9; Marx, 2012, p. xxv). Overly broad definitions can lead to surveillance becoming normalised as a routine part of everyday life. Such routinisation will most likely lead to 'surveillance realism' (Dencik and Cable, 2017, pp. 763–81) setting in, resulting in publics accepting their fate and failing to organise against it (Fuchs, 2010, pp. 1–22; Duncan, 2018, pp. 28–36). This narrowed definition does not negate the fact that contemporary surveillance often operates in highly complex, distributed ways, but recognises that such a surveillant assemblage can, in fact, enhance social control in that it can extend the capabilities for intelligence-driven surveillance.

We understand intelligence to be knowledge of an adversary using all sources of information, including those that may have been gained by clandestine means, and aimed at protecting collective security to prevent an adversary from causing harms of major significance to it. This definition avoids one of the major dangers of intelligence, which is to define the term too broadly, leading to intelligence agencies being provided with mandates that intersect with, and even replace, other policy areas. It also avoids state-centric definitions (see, for example, the definition offered by Warner (2002, pp. 15–22) as secret state activity designed to understand or influence foreign entities) by recognising implicitly that a broader range of actors can practise intelligence. Such was the case during emancipatory struggles across Southern Africa, where national liberation movements formed their own intelligence capabilities. Beyond the more conventional roles of preventing violent attacks and other threats of national significance, increasingly governments are requiring intelligence agencies to ensure that policymakers enjoy decision advantages, by providing them with relevant conflict-winning information over issues that are vital to the welfare of the country. These additional tasks have become incorporated into definitions of intelligence that emphasise its role in supporting national interests, especially economic interests such as trade advantages, particularly on the global stage, and not just protecting against threats. Once intelligence mandates include not just threats, but interests too, including economic interests, then all manner of abuses become possible and even likely (Hager, 1996, pp. 241–3; Duncan, 2022, pp. 14–18).

We understand intelligence oversight to mean the superintendence of intelligence in a manner that is independent from the everyday management and practices of intelligence and the institutions that collect, analyse and store it (Caparini, 2007, p. 3). Exercising oversight is the key to ensuring accountability (Hotzel, 2014; Moser, 2018). Hotzel (2014) notes that oversight, in governance terms, means 'watchful care', that is, society keeping an eye on certain processes, their implementations, and the plans and decisions that, in the first instance, led to them. The intention of such oversight is to ensure that intelligence practitioners comply with their mandates, with controversies remaining over whether overseeing should be post hoc or extend to the authorisation of covert actions before they occur (Gill and Phythian, 2012, p. 173). Oversight is a precondition for intelligence accountability, where practitioners are required to explain and justify their actions (Gill 2020), deliver effective intelligence, prevent intelligence failures and build public trust (Goldman, 2016, pp. 207–34). Accountability is a counterweight to the exercise of public power on the basis of formal and informal procedural and institutional arrangements. Those who hold power should be and are, expected to explain and justify its use (Moser, 2018). The threat or shadow of sanctions can indeed influence the behaviour of actors who are aware of the fact that their conduct or performance will be analysed and, eventually, evaluated by an accountability forum. Ensuring effective accountability is likely to include demands for radical transparency in how surveillance operates that move beyond mere demands for disclosure of information (McCarthy and Fluck, 2016). Instead such transparency would need to tackle the social conditions that allowed interactions between intelligence agencies and publics to become so asymmetric and disempowering, and empower these publics with the capabilities needed to act if their demands for information are successful.

The liberal democratic ‘ideals’ of intelligence oversight

Democratic oversight of intelligence is meant to be an alternative to more authoritarian systems, where governments or dominant political parties may exercise stewardship over agencies. Such systems may lack any oversight structures at all or, where they exist, they are likely to be extensions of the authoritarian system rather than providing checks on it. Democratic oversight promises to check intelligence excesses and prevent surveillance overreach to ensure that intelligence agencies fulfil the broader public interest, as opposed to sectional, partisan interests.

The liberal democratic accounts of oversight that dominate intelligence literature are animated by certain guiding principles. These include ensuring that intelligence agencies respect the rule of law, where governments use laws and policies to limit state power to conduct stewardship. While recognising the need for secrecy in relation to legitimate intelligence methods, these agencies need to operate with some degree of openness and transparency. Accountability to the public through their elected representatives, and usually through a parliamentary committee, is also another key principle. The bodies that practise oversight are also meant to be independent of the agencies they oversee, have access to the information needed to facilitate effective oversight, and conduct regular reviews. There are also meant to be checks and balances between the different spheres of government to guarantee this independence and they communicate their findings to the public while maintaining legitimate secrecy. As an additional check, some countries have also institutionalised the practice of including opposition parties in intelligence briefings, to prevent capture of intelligence by ruling parties (Leigh, 2006, pp. 70–1).

In terms of its basic architecture, intelligence oversight for national security purposes is meant to cover all areas of intelligence activities, but not be reduced to micromanagement (Gill, 2020, p. 973), and can start at the executive level, taking the form of guidelines or ministerial directions, as ministers are not meant to become involved in day-to-day operations of the agency they oversee (Caparini, 2007, p. 10–11). Requiring intelligence agents to report illegal actions can also provide important information for executive oversight (Born et al., 2005, p. 46). However, in a field where executive authority is traditionally strong (Goldman, 2016, p. xvii), the executive alone cannot be relied on to police intelligence agencies, as the politicians responsible for executive oversight may have a vested interest in keeping surveillance overreach secret, to protect themselves from potentially politically damaging scandals about surveillance overreach (Goldman, 2016, p. xiv).

Other state institutions that are meant to be independent of intelligence agencies can also exercise oversight and can include the judiciary, ombuds or Inspector General offices and oversight committees. Judges can direct agencies to undertake or refrain from certain actions or oversee agencies through after-the-fact inquiries and are more likely to focus on the propriety or legality of agency actions, while parliamentary committees are likely to focus on their efficacy (Caparini, 2007, p. 3), with judicial oversight functioning effectively only when there is an independent judiciary and proper controls inside agencies (Caparini, 2007, p. 15). Parliamentary committees may be established that are responsible for adopting intelligence budgets, passing intelligence legislation and interrogating reports from agencies (Johnson, 2018, pp. 31–68; Caparini, 2007, pp. 12–13). Parliamentary oversight is important to cement civilian control of intelligence, thereby preventing militaries misusing intelligence for internal repression of dissent (Caparini, 2007, p. 3). Some countries have established single parliamentary committees to oversee all intelligence agencies, ensuring that knowledge and expertise on intelligence is retained in the same committee, some may be restricted to scrutinising matters of policy and law while others may enjoy powers to inquire into operational matters, with the former more likely to hold hearings in public than the latter (Leigh, 2006, pp. 71–2).

The existence of several layers of oversight is meant to ensure that higher levels of oversight will step in and compensate for any failures at a more subsidiary level. Ombuds or Inspector General offices, for example, could strengthen executive oversight by reporting to parliament on any failures in executive control. Parliaments, which may supposedly be at the centre of democratic oversight as they consist of elected representatives may, in fact, lack the ability to conduct investigations of their own, despite having legislative responsibility for oversight, and having administrative oversight bodies that are tasked with doing just that, assist them to detect wrongdoing that may otherwise remain secret, even to them. The oversight agencies themselves are typically legislated into being, with powers and responsibilities being set out in law and policy, and these responsibilities may extend beyond oversight entities considering the legality of intelligence actions but their propriety too, where their ethical conduct is considered (Gill and Phythian, 2012, p. 175).

Governments may also establish ad hoc committees of inquiry, particularly in the wake of a significant intelligence failure or surveillance scandal, and these too can provide an additional layer of oversight. In providing a concentrated focus on a specific issue, they can generate valuable findings, command significant media attention and galvanise the public. However, to do so, the inquiry's members would need to be independent from vested interests, their procedures would need to be robust, and they would need to operate as transparently as possible.

Systemic failures in oversight: Bringing the public back in

The liberal democratic 'ideal' of intelligence oversight provides a basic schema for how intelligence oversight is meant to operate. However, as became apparent from the Snowden revelations, it has failed to keep up with the growth in digital surveillance capabilities. It is too easy to blame lapses on the failings of individual spies instead of structural biases in how intelligence operates and systemic failures in how oversight functions, as Loch K. Johnson has argued:

> Neither the inability to predict future events with precision . . . nor the acknowledgement that secret government organisations can be a danger to open societies . . . should astound. After all, intelligence agencies are comprised of human beings – flawed by nature and devoid of a crystal ball; consequently, one can anticipate failures and abuses (Johnson, 2012, p. 6).

By individualising and exceptionalising abuses, explanations of intelligence failures and abuses risk sidestepping difficult questions about how oversight may have been structured to evade accountability. Mechanisms that have been set up, such as parliamentary committees or Inspector Generals for Intelligence, often struggle to hold the agencies they oversee accountable, and they may even be captured by these very institutions. Attempts to rein in intelligence abuses have, all too often, focused narrowly on reforms, such as improving internal controls, strengthening oversight institutions such as parliament and ombudsman, improving training and clarifying mandates. This narrow focus has led to a proliferation of oversight institutions that have not challenged sufficiently the legitimacy of modern intelligence as it is understood and practised. Typically, these oversight bodies are inadequate and continue to treat state spying on activists and journalists, infiltration of social movements and the like, as departures from what these agencies do, rather than being integral to what they do (Choudry, 2018, pp. 3–16). Judges can become captured by the very agencies they are meant to oversee and fail to take independent decisions (Gill, 2020, p. 972). Official oversight bodies may become inscribed into a circle of secrecy, where they become integrated into secretive intelligence culture, particularly if the senior officials who staff these agencies come from the very institutions that are being overseen. Therefore, the mere existence of formal oversight bodies may not prevent the growth of accountability gaps, and greater corporate involvement in intelligence is making the problem worse (Gill, 2020, p. 983), with the gaps likely to be more pronounced in so-called 'transitional societies' in the global south (Caparini, 2007, p. 21).

Accountability gaps have become even more pronounced in relation to digital surveillance, as oversight based on supervision of the national sphere of government and state intelligence activities has proved to be inappropriate in an era when intelligence is practised increasingly on a decentralised and transnationalised basis. Intelligence is also practised increasingly through public–private partnerships or by private contractors and these changes have led to intelligence capabilities outstripping the abilities of their overseers (Goldman, 2016, pp. xx–xxiii; Gill, 2020, p. 983).

The repeated failures of formal oversight to prevent intelligence abuses could be attributed to naïve assumptions about representative democracy being a substantive expression of 'the will of the people', held in check by the supposed rationality of bureaucratic power, but which can all too easily boil down to government by elites. These ideals are unlikely to be sufficient to ensure substantive intelligence accountability, which may well need to be animated by more participatory forms of democracy that can occur in contrast to, and even in defiance of, the formal institutions of representative democracy. Consequently, real moments of effective intelligence oversight have occurred through public mobilisation, using strategies such as litigation, advocacy and whistleblowing (Kniep et al., 2023, p.2). In the wake of the Snowden disclosures, whistleblowing has received more attention. By virtue of their proximity to classified information, whistleblowers can expose intelligence abuses, but they can do so only if they are protected and not persecuted. This may be the case especially in situations where internal organisational cultures rest on codes of professional ethics that require adherence to the highest standards of conduct (Caparini, 2007, p. 11).

When the media, NGOs and citizens are acknowledged as part of the oversight system, their role often seems secondary to the main discussion about oversight structure. However, these groups can support parliaments in their oversight duties by highlighting abuses through research, journalism, legal action and advocacy (Gill and Phythian, 2012, p. 175). Their roles in exposing intelligence scandals when they occur – what Loch K. Johnson refers to as a shock theory of intelligence accountability, where intelligence scandals or alarms lead to intense bursts of intelligence accountability (Johnson, 2018, pp. 209–46) – can lead to lasting changes to intelligence law, policy and practice. Their success often depends on their ability to generalise claims about injustice, which many social actors have failed to do when confronted with major, generalised government claims around national security, and where their counterarguments may be in defence of singular groups or rights (Aradau and McCluskey, 2022, pp. 1–19).

But who exactly is the public? How publics have been constituted differ from one context to another and depends largely on the politics of the day (Ku, 2000). For example, in more liberal and democratic contexts, public oversight of state institutions may not only be tolerated, but encouraged (Brennan Centre for Justice, 2021). But the question would be: who exactly constitutes 'the public' that we are talking about? Some of the earliest conceptualisations of 'the public' in Africa (for example, Mamdani (1996) dichotomise them into two: the elite (the citizens with power) and the subjects (those acted upon by power)). In this book, we understand the public in a rather clear and straightforward sense. For a start, we use the term 'the public' in this book only in reference to intelligence oversight. We, therefore, mean citizen agency, meaning those citizens who are not part of the institutions tasked with surveillance. We also mean those who are not part of the policy-making circles. This means, rather in a paradoxical sense, citizens who are constituted to provide a layer of oversight on data-driven intelligence. In other research, public oversight has been interpreted to mean community oversight of surveillance (Cole, Eppert and Kinzelbach, 2008). Public oversight, hence, means a broad coalition of local groups and activists working to end the unchecked surveillance of communities by local agencies – including law enforcement and military and civilian intelligence – and to ensure that people have a say in whether, what, and how surveillance technology is acquired and used in their country or locality. In all this myriad of interpretations of what exactly constitutes the public, there are key points of convergence about this question. Firstly, the public are 'outsiders'. In other words, they are civilians who have little or no connection to the agencies of surveillance which they should watch over. Secondly, they are civilians (Ku, 2000) exercising independent agency on surveillance practices and institutions. Thirdly, they have one major objective – to hold institutions accountable for the work they do, ensure they do it within the limits and provisions of the law, and safeguard civilian rights and fence them off from intrusion by surveillance institution. When this objective is met, it, possibly, can bridge the distrust between the institutions of surveillance and the communities of the surveilled.

However, and as Mamdani (1996) alludes to, publics in Southern Africa are deeply divided along the lines of class, race, gender and other social fault lines. They may be constituted in elite ways that claim to represent the public, but in reality, represent organisations with no real social base. Others may be constituted in more mass-based, popular ways. Under certain conditions, and if pushed far enough by public pressure, private companies may switch sides and defend citizen privacy if it is in their business interests to do so, thereby contributing to public oversight. So, apart from examining how privatisation of intelligence functions has contributed to the weakening of official oversight, and presented new challenges for public oversight, the chapters will also examine the following questions: under what conditions can the private sector contribute to public oversight rather than evading it?

In short, the chapters interrogate how publics have been constituted for surveillance oversight, which forms of mobilisation have had lasting, positive effects and which forms have been less successful.

Outline of chapters

The chapters in this edited volume include contextual information about the country's intelligence agencies, how they are organised and their oversight, as well as (to the extent that is possible, given the often secretive nature of the information) information about their capabilities for surveillance. The articles will focus on drawing out the lessons for public oversight, particularly as they relate to digital surveillance practices or practices with considerable surveillance potential. The practices examined in these chapters are diverse, and include smart cities and surveillance (Mauritius); state intelligence surveillance and its oversight (Botswana); targeted surveillance and oversight (Angola, Zimbabwe and the DRC); transnational signals intelligence surveillance and its oversight (Mozambique and South Africa); SIM-card and mobile-device registration and public responses (DRC, Namibia and Mozambique) and biometric surveillance in the context of identity management (Mauritius). The chapters then proceed to illuminate different elements of public oversight, and what it takes to build it, sustain it and make it effective. This book makes several but closely related arguments. The broader argument we sustain throughout the interlinked chapters is that, beyond judicial and executive surveillance models that are common, a new model of public oversight of surveillance is possible and, arguably, functions better than extant approaches to surveillance. In making this argument, our starting point is that extant oversight mechanisms have declined in efficacy and in some other contexts, been circumvented by partisan institutions. There is, hence, the need for a new model of oversight, especially one that is novel enough to include civilians. A publicly driven model, which we will outline some essential elements of in the concluding chapter, would likely increase transparency of intelligence surveillance and substantive accountability. It can do this by providing another layer of oversight existing independently from, and at times even in antagonism to, state/corporate power. Each chapter of this book sustains this argument in several ways.

Rui Verde explores the role of international pressure in public oversight, to compensate for a grossly inadequate formal oversight of state intelligence in Angola, which he characterises as an anocratic regime. As he discusses, such a regime, is neither completely open to political contenders due to autocratic tendencies nor is it completely closed to moments of democratic opposition. Such a moment occurred in relation to the 15+2, or Luanda Reading Club case, touched on earlier. Verde shows how public oversight forced the hasty approval by parliament of an amnesty law after a massive international outcry at their conviction. Verde also explores whether or not international pressure opened up meaningful spaces for local activism.

In the case of Botswana, Tachilisa Badala Balule explores the role of public oversight driven by popular agency of a constellation of civil society and social-movement actors and is another example of successful public oversight. While local networked activism was more of a feature in this case than in the Angolan case, it has yet to translate into more nationally sustained oversight, but nevertheless the potential is there. Balule discusses how the controversies around the Criminal Procedure and Evidence Bill mentioned earlier, led to the government having to walk back some of the worst elements of the Bill that threatened basic democratic rights and freedoms. There is, however, evidence that popular agency oversight over the security sector in the country remains limited despite this victory, and the question Balule attempts to answer is, why?

Trésor Maheshe Musole examines the factors that militate against successful public oversight in the DRC, and seeks to answer two questions: what are the explanatory factors for the low interest of Congolese civil society in the issue of surveillance and how could civil society actions limit the abuses of surveillance? The chapter utilises two cases – one successful and relating to opposition to the registry of mobile devices, and the other unsuccessful and relating to the surveillance of public figures – to account for low monitorial interest on the part of civil society organisations and suggests ways through which the public, through organised formations, can be engaged in action that limits surveillance abuses. By analysing these two cases, the chapter clearly articulates how public oversight can be successful, and the inhibiting factors that can make it fail.

Sarah Chiumbu discusses the factors influencing public oversight of digital surveillance in Mauritius, which provides arguably the most impressive example of local activism discussed in this edited volume, and one that has reduced the scope for surveillance overreach on a more sustained basis as popular consciousness of the dangers remain embedded in the social fabric. Chiumbu discusses how in 2013 the Mauritian government introduced the smart ID card to replace the previous National ID Card as a public-public partnership with Singapore, and how through opposition from the public, activists and civil society organisations, who were concerned that the government could use this information for surveillance purposes or to track the activities of citizens, the government suspended the project in 2015. It looks at why sections of the public were open to being mobilised and how a popular campaign around surveillance can be built and achieve lasting gains, and emphasises the importance of relating surveillance to bread-and-butter issues.

Ernesto Nhanale and Borges Nhamirre offer a much more sombre analysis of the structural environment for the failing of oversight mechanisms in Mozambique, both formal and public. They examine the continuities between colonial authorities and the post-liberation state as a key factor that has limited scope for meaningful oversight. They argue that the absence of such oversight mechanisms could be attributed, not only to the political culture of colonial control continuing into the post-colony, reaching deep into society and exacerbated by military conflicts, but also to an institutional and legal model with its roots deep in colonialism, and which the government is still reluctant to restructure. This reluctance is an important factor in the maintenance of Frelimo as the only actor in the political system and national governance.

Frederico Links and Phillip Santos explore the systemic failure of digital surveillance oversight of the Namibia Central Intelligence Service (NCIS), despite the country being touted as a postcolonial democratic success story. They explore how official oversight has been set up to fail and, consequently, how the media have stepped into the breach and used judicial activism to roll back the culture of secrecy around surveillance. Links and Santos utilise a critical incident to make their argument. In August 2018, in the High Court of Namibia, lawyers acting on behalf of the NCIS and the Namibian government argued on the record that the intelligence agency should 'be insulated from both parliamentary and judicial oversight'. This they did as part of their attempt to prevent a local newspaper from revealing evidence of corruption and mismanagement in the NCIS. However, the NCIS lost the case.

Jane Duncan explores the difficulties of maintaining public oversight over surveillance. She uses a successful campaign in South Africa as a case study to illustrate her points. She examines the campaign around a controversial 'Secrecy Bill', which was broadened to focus on the inappropriately large roles of surveillance, intelligence and security institutions in the governance of contemporary society, and why it could not be sustained. Through the lens of political process theory underpinned by a critical approach, this chapter examines the factors that contributed to the rise and fall of anti-surveillance activism in South Africa. She shows how the anti-surveillance activism that was taken forward in the wake of the campaign, was done so in less mass-based and more elitist ways, such as strategic litigation in the absence of a mobilisation strategy, which has led to the considerable capacity that has been built in civil society struggling to curtail surveillance powers on an ongoing basis.

Allen Munoriyarwa seeks to envision a new civilian-driven model for countering state authoritarianism in surveillance regulation bolstered by private actors, especially from China and Iran, using two surveillance scandals in Zimbabwe as the backdrop. He explains how Zimbabwe is contending increasingly with a slew of digital surveillance practices ranging from location surveillance, digital communication, public-space surveillance and many more. Drawing on the critical-incidents method and on limited interviews with civic-society actors, legislators and activists, Munoriyarwa seeks to answer three questions: to what extent can the state lead a transparent and effective surveillance regime which does not, by design or by accident, unnecessarily infringe on individual privacy; how can surveillance institutions be held accountable for their actions; and, lastly, what pathways exist to bolster collective civilian inclusion in surveillance regulation?

In the concluding chapter, Jane Duncan and Allen Munoriyarwa tie up the arguments made in the book. They reflect on the current trajectories of intelligence surveillance in the region, and What it is likely to morph into both the long and the short term. In addition to this, they also reflect on the elements of a publicly driven models of intelligence oversight, drawing on the evidence presented in the chapters. Doing so allowed them to start developing a theoretical basis to predict conditions in which public oversight is likely to succeed.

As the editors, we hope that this book will be of immediate benefit to some of the most socio-economically deprived countries in the world, where the risks of using surveillance powers to stabilise existing power structures, instead of addressing the root causes of inequality, are high. We also believe that the lessons to be learnt from these countries are of global relevance because bottom-up change is more likely to occur in political systems with less social consensus and consequently more political ferment.

References

Aradau, C. and McCluskey, E. 2022. Making digital surveillance unacceptable? Security, democracy, and the political sociology of disputes. *International Political Sociology*, 16, pp. 1–19. [Online]. [Accessed 20 July 2023]. Available from: https://doi.org/10.1093/ips/olab024.

Balule, B.T. and Dambe, B.J. 2023. Surveillance within the law: A critique of the legal framework for surveillance of digital communications by Law Enforcement Authorities in Botswana. *Statute Law Review.* 44(2), pp. 1–14.

Bellamy Foster, J. and McChesney, R. 2014. Surveillance capitalism: Monopoly-finance capital, the military-industrial complex, and the digital age. *Monthly Review.* 66(3).

Born, H., Johnson, L. and Leigh, I. 2005. *Who's watching the spies?: Establishing intelligence services accountability.* Sterling, VA: Potomac Books.

Bovens, M.W, Thomas, S. and Goodin, E. 2014. Public accountability. In: Goodin, T. ed. *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press, pp. 114–120.

Brennan Center for Justice. 2021. The public oversight of surveillance technology (POST) Act: A resource page. [Online]. [Accessed 24 August 2023]. Available from: https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page.

Caparini, M. 2007. *Democratic control of intelligence services: Containing rogue elephants.* Aldershot: Ashgate.

Choudry, A. ed. 2018. *Activists and the surveillance state: Learning from repression.* London: Pluto Press.

Clarke, R. 1988. Information technology and dataveillance. *Communications of the ACM*. 35(5), pp. 498–9.

Cole, E., Eppert, K. and Kinzelbach, K. 2008. *Public oversight of the security sector: A handbook for civil society organizations.* UNDP Bratislava Regional Centre; Geneva Centre for the Democratic Control of Armed Forces (DCAF). [Online]. [Accessed 10 August 2023]. Available from: https://www.undp.org/publications/public-oversight-security-sector-handbook-civil-society-organizations.

Couldry, N. and Mejias, U.A. 2019. Data colonialism: Rethinking big data's relation to the contemporary subject. *Television and New Media.* 20(4), pp. 336–49.

Dencik, L. 2018. Surveillance realism and the politics of imagination: Is there no alternative? *Krisis: Journal for Contemporary Philosophy*. 1, pp. 31–43.

Dencik, L. and Cable, J. 2017. The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*. 11, pp. 763–81.

Duncan, J. 2022. *National security surveillance in Southern Africa: An anti-capitalist perspective*. London: Bloomsbury Academic & Professional.

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

Esser, F. 2019. Comparative research. In: Van den Bulck, H., Puppis, M., Donders, K and Van Audenhove, L. eds. *The Palgrave Handbook of Methods for Media Policy Research.* Palgrave Macmillan, pp. 85–101.

Fuchs, C. 2010. How can surveillance be defined? Unified Theory of Information Research Group. *The Internet and Surveillance Research Paper Series,* 1, pp. 1–22. [Online]. [Accessed 2 August 2023]. Available from: http://www.sns3.uti.at/wp-content/uploads/2010/10/The-Internet-Surveillance-Research-Paper-Series-1-Christian-Fuchs-How-Surveillance-Can-Be-Defined.pdf.

Gill, P. 2020. Of intelligence oversight and the challenge of surveillance corporatism. *Intelligence and National Security.* 35(7), pp. 970–89. doi: 10.1080/02684527.2020.1783875.

Gill, P. and Phythian, M. 2012. Intelligence in an insecure world. Cambridge: Cambridge University Press.

Giroux, H.A. 2015. Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies*. 29(2), pp. 108–40.

Goldman, Z.K. 2016. The emergence of intelligence governance. In: Goldman, Z.K. and Rascoff, S.J. eds. *Global intelligence oversight: Governing security in the twenty-first century*. New York: Oxford Academic, pp. 207–34.

Granick, J.S. 2017. *American spies: Modern surveillance, why you should care, and what to do about it*. Cambridge: Cambridge University Press.

Hager, N. 1996. *Secret Power.* Nelson: Craig Potton Publishing.

Hintz, A., Dencik, L. and Wahl-Jorgensen, K. 2019. *Digital citizenship in a datafied society*. Cambridge: Polity Press.

Hotzel, S. 2014. The concept of oversight, its connection to memory keeping and its relevance for the medium term: the findings of the RK&M Initiative. Constructing Memory – International Conference & Debate on the Preservation of Records, Knowledge and Memory Across Generations. Verdun, France: 15–17 September 2014.

Johnson, L.K. 2012. *National security intelligence*. Cambridge: Polity Press.

Johnson, L.K. 2018. *Spy watching: intelligence accountability in the United States.* Oxford: Oxford University Press.

Kniep, R., Ewert, L., Reyes, B., Tréguer, F., Cluskey, E. and Aradau, C. 2023. Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies.* pp. 1–21. doi:10.1017/S0260210523000013.

Ku, A.S. 2000. Revisiting the notion of 'public'. *Sociological Theory*. 18(2), pp. 216–40.

Leigh, I. 2006. The accountability of security and intelligence agencies. In: Johnson, L.K. ed. *Handbook of intelligence studies*. Abington: Routledge, pp. 67–81.

Lyon, D. 1994. *The electronic eye: the rise of the surveillance society.* Minneapolis: University of Minnesota Press.

Lyon, D. 2015. Keynote presentation to the International Association for Media and Communications Research, 14 July 2015. [Online]. [Accessed 15 July 2023]. Available from: https://www.youtube.com/watch?v=Vzgok3kUl0o.

Lyon, D. 2018. *The culture of surveillance: watching as a way of life.* Cambridge: Polity Press.

Mamdani, M. 1996. *Citizen and subject: contemporary Africa and the legacy of late colonialism.* Princeton: Princeton University Press.

Mann, M. and Daly, A. 2019. (Big) data and the north-in-south: Australia's informational imperialism and digital colonialism. *Television and New Media*. 20(4), pp. 379–95.

Marx, G. 2012. 'Your papers please': Personal and professional encounters with surveillance. In: Ball, K., Haggerty, K.D. and Lyon, D. eds. *Routledge handbook of surveillance studies*. Oxford: Routledge, pp. xx–xxxi.

McCarthy, D.R. and Fluck, M. 2016. The concept of transparency in International Relations: Towards a critical approach. *European Journal of International Relations*. 23(2), pp. 416–40. [Online]. Available from: https://doi.org/10.1177/1354066116651688. Accessed 5 July 2023.

Micova, B.S. 2019. Case study research. In: Van den Bulck, H., Puppis, M., Donders, K. and Van Audenhove, L. eds. *The Palgrave Handbook of Methods for Media Policy Research*. Cham: Palgrave Macmillan, pp. 71–84.

Moser, C. 2018. Conceptualising accountability in the legal and institutional framework of the OSCE. Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper. [Online]. [Accessed 20 August 2023]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228528.

Munoriyarwa, A. and Mare, A. 2022. *Digital surveillance in Southern Africa*. Cham: Palgrave Macmillan.

Ndlovu, T. 2022. Botswana civil society rebuff Criminal Procedures Bill. Association for Progressive Communications. 23 August. [Online]. [Accessed 5 July 2023]. Available online: https://www.apc.org/en/news/botswana-civil-society-organisations-rebuff-criminal-procedures-bill.

Pillar, P. 2010. The perils of politicisation. In: Johnson, L. ed. *The Oxford handbook of national security intelligence*. Oxford: Oxford University Press, pp. 472–84.

Saul, J. 2005. *The next liberation struggle: Capitalism, socialism and democracy in Southern Africa*. Toronto: Between the Lines.

Schedler, A., Diamond, L.J. and Plattner, M.F. eds. 1999. *The self-restraining state: power and accountability in new democracies*. Boulder, CO: Lynne Rienner Publishers.

Shiraz, Z. and Aldrich, R.J. 2019. Secrecy, spies and the global South: Intelligence studies beyond the 'Five Eyes' alliance. *International Affairs*. 95(6), pp. 1313–29. [Online]. [Accessed 20 July 2023]. Available from: https://doi.org/10.1093/ia%2Fiiz200.

US House of Representatives. 2016. Review of the unauthorised disclosures of former National Security Agency contractor Edward Snowden. [Online]. [Accessed 10 January 2024]. Available from: https://www.congress.gov/committee-report/114th-congress/house-report/891/1.

Van Puyvelde, D. 2013. Intelligence accountability and the role of public interest groups in the United States. *Intelligence and National Security.* 28(2), pp. 139-158, Available from: https://doi-org.ezproxy1.lib.gla.ac.uk/10.1080/02684527.2012.735078.

Van Puyvelde, D. 2018. Qualitative Research Interviews and the Study of National Security Intelligence. *International Studies Perspectives*. 19(4). November, pp. 375–391. [Online]. [Accessed 1 August 2023. Available from: https://doi-org.ezproxy1.lib.gla.ac.uk/10.1093/isp/eky001.

Verde, R. 2021. *Words and actions: a realistic enquiry into digital surveillance in contemporary Angola.* Johannesburg: Media Policy and Democracy Project. [Online]. [Accessed 15 August 2023]. Available from: http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/report_03_2021_words_and_actions_angola_masterset.pdf.

Voltmer, K. and Kraetzshmar, H. 2015. *Investigating the media and democratisation conflicts: Research design and methodologies of media, conflict and democratisation*. Media Conflict and Democratisation (MeCoDEM). [Online]. Accessed 12 July 2023. Available from: https://eprints.whiterose.ac.uk/id/eprint/117317/1/VoltmerKraetzschmar-2015_Investigatingmediaanddemocratisationconflicts.pdf.

Warner, M. 2002. 'Wanted: A Definition of Intelligence'. *Studies in Intelligence.* 46(3).

Wegge, N. and Wentzling, T. 2018. Contemporary and Future Challenges in Effective Intelligence Oversight. In: Leigh, I., & Wegge, N. Eds. *Intelligence oversight in the twenty-first century: accountability in a changing world* (1st ed.). Oxford: Routledge. https://www.routledge.com/Intelligence-Oversight-in-the-Twenty-First-Century-Accountability-in-a/Leigh-Wegge/p/book/9780815393344.

Yong Jin, D. 2015. *Digital platforms, imperialism and political culture.* Oxford: Routledge.

Zuboff, S. 2019. *The age of surveillance capitalism.* London: Profile Books.

CHAPTER TWO

Intelligence-driven digital surveillance and public oversight success in an anocracy: Angola and the 15+2 case

Rui Verde

Introduction

This work focuses on an example of successful public oversight in the anocratic political context of Angola. It assesses how public oversight of intelligence-driven digital surveillance can stop a government from abusing its capabilities and argues that in specific situations international pressure can compensate for limited opportunities for national mobilisation, with positive implications for sustaining national public oversight. It centres on a famous case, known as the 15+2 case, or the Luanda Reading Club.

The elaboration of the chapter was based in part on the personal experience of the author who at the time directly followed the events for professional reasons, on various news material published, and on 21 interviews with relevant persons (members of the 15+2 group; journalists, lawyers, former members of the security services) conducted in 2023 and 2024 with the substantial collaboration of José Luís Domingos and Tânia Canguia, from the Center for Research in Law at the Catholic University of Angola, who participated in this research, and to whom a public acknowledgement is due.

Contrary to what could be expected, we did not find any obstacles from the authorities in developing our work. The difficulty was encountered in some of the interviewees' attitudes of self-censorship.

Angola: The context

Angola is not a democracy, but neither is it a dictatorship. Its regime is the result of a complex historical process. In 1961, the fight against Portuguese colonialism began. Angola was colonised by the Portuguese from the sixteenth century onwards. Initially, colonisation proceeded along the coast but over the centuries, and especially from the second half of the nineteenth century, it expanded into the hinterland, facing strong armed resistance from various native populations. It was only around the 1920s that the country was considered 'pacified' by the Portuguese (Oliveira Pinto, 2015). For a short time, as from the 1950s onwards, resistance movements were organised and consequently armed struggle against Portugal started afterwards. This was a divisive struggle, with liberation movements combating Portugal and fighting among themselves (Oliveira Pinto, 2015), also resulting in the establishment by the Portuguese authorities of a strong security apparatus. Mostly, three liberation movements were operational, although on a small scale, when a democratic revolution occurred in Portugal on 25 April 1974. These movements were *Movimento Popular de Libertação de Angola* (MPLA), *Frente Nacional para a Libertação de Angola* (FNLA) and *União Nacional para a Independência Total de Angola* (UNITA).[1] Although these movements had the same objective – the independence of Angola – their differences were quite pronounced and became more entrenched over time, with disastrous results in terms of political and social tension. The MPLA was essentially formed by intellectuals with Marxist tendencies, many of whom had undergone higher education in Portugal, such as Agostinho Neto, the future

[1] Translated as the Popular Movement for the Liberation of Angola (MPLA), the National Front for the Liberation of Angola (FNLA) and the National Union for the Total Independence of Angola (UNITA).

President of the Republic, who graduated in medicine from the University of Coimbra. It quickly aligned itself with the Soviet Union and was sponsored by it and its allies. The FNLA, on the other hand, was based on the Bakongo ethnic group from northern Angola, had strong ties to Mobutu's Zaire and was supported by the US. Finally, UNITA, which began as a dissident group of the FNLA, ended up representing the largest ethnic group in Angola, the Ovimbundu. Although the ethnic aspects underlying the movements should not be overemphasised, in terms of public perception, antagonistic images were created, with the MPLA representing the city, urbanity and some miscegenation, and UNITA representing the deep country rurality and a streak of tribalism.

Afterwards, history accelerated and independence was obtained in 1975, followed by a long, sporadic civil war between 1975 and 2002. Soares de Oliveira (2015) summed up the war in an incisive way, writing, 'The conflict, which killed up to a million people, was tightly linked with international dynamics, such as the struggle against colonialism and apartheid, the Cold War and commercial appetite for petroleum and diamonds' (p. 1).

Civil war had always been a potential threat since the beginning of the Angolan armed struggle in the 1960s, as the movements opted for different strategic alliance and represented different *Weltanschauungs* and ethnicities, as seen above, beyond the existing personal animosities between the leaderships. The MPLA gradually became strongly Marxist and played a leading role in advancing Soviet ambitions in the region. It had, after the 1974 Portuguese revolution, the complicity of the new Portuguese authorities, who were themselves partly aligned with the Portuguese Communist Party and in coordination with Moscow. UNITA had already established some tactical alliances with the previous Portuguese authorities and, together with the FNLA, presented itself as aligned with the West. Thus, Angola, rich in oil, quickly became a chessboard for the great powers (Marques, 2013).

After obtaining political power in Luanda in 1975, the MPLA was never to let it go. First, it installed a Marxist regime that adopted a pro-Soviet Constitution (Bacelar Gouveia, 2014). Then, after more than 15 years of civil war, through an agreement with its rival, UNITA, it adopted a constitutional law following a liberal democratic pattern in 1991/1992. This agreement occurred after the end of the Cold War. In fact, the MPLA was losing its main support – the Soviet Union – which dissolved itself in December 1991, and the US, for a time, abandoned interest in maintaining prolonged conflicts, since it no longer had an enemy. Thus, the Angolan movements saw their external sponsors disappear. This, and a weariness of a prolonged state of war, probably led to the attempt to reach an agreement.

The first elections in the country were held in September 1992. However, the electoral process never produced final results as the civil war was rekindled. Only with the death of Jonas Savimbi, the leader of UNITA, in 2002 was peace achieved (Soares de Oliveira, 2015). José Eduardo dos Santos of the MPLA, then president of the republic (since 1979, when he succeeded the founder, Agostinho Neto, also from MPLA), took his time to call elections, which only took place in 2008. Since that year the country has had reasonably free elections, although their fairness has always been strongly disputed (Verde, 2021). Elections took place in 2008, 2012, 2017 and 2022, with the MPLA the winner of each, although the scale of its victories declined progressively. In 2008 it obtained around 81 per cent of the votes; in 2012, 71 per cent; in 2017, 61 per cent; and in 2022, 51 per cent. Therefore, although the MPLA won convincingly, the results did not mirror those of a pure dictatorship and apparently showed a reasonable projection of popular will. This means that there will be a space for public oversight in this kind of regime.

Angola has a democratic Constitution (2010) based on the Portuguese one, although it has some traits of the Constitution of the United States of America, mostly in terms of executive power (Bacelar Gouveia, 2014). Constitutionally, the Angolan security apparatus, composed of the State Intelligence and Security Service (SINSE), the Military Intelligence and Security Service (SISM) and the External Intelligence Service (SIE), are auxiliary bodies of the President of the Republic, to whom they provide assistance in his/her executive function.

Parts of the Constitution are feebly enforced, mostly with regard to fundamental rights, since the Constitutional Court is generally deferential to the executive branch (Verde, 2021). While demonstrations are allowed by law, they are sometimes forbidden in practice, and although freedom of expression is guaranteed, some people are jailed due to defamation laws (Verde, 2021). This ambivalence between text and fact – democracy and authoritarianism – is ever present in Angola. Since the mid-nineteenth century, Angola has been living this reality of differentiation between law and fact. At the time, the contrast between the abolitionist laws on slavery and the reality on the ground were blatant, as the economy was essentially based on slavery. Its abolition by the law was not complied with in practice, which led to the coining of the term *para Inglês ver* (for the English to see). Anti-slavery laws were adapted simply to please the English but they were not applied daily, or were applied intermittently. This surreptitious legal culture probably continued, and was accentuated again when, in 1991/1992, a government and a party with an authoritarian Marxist background transformed itself, in a fortnight, into a social-democratic party and adopted the norms of a democratic constitutional system, without the respective structures having been reformed or even adapted.

Among the population percolates the idea that Angola's institutions and political parties were designed for an environment of war and confrontation, having conflict at their core, and that they are incapable of dealing with a new Angola in which the central objectives are the development and well-being of the population, as shown by last public surveys (Afrobarometer, 2024).

This means that the 'old' parties are no longer considered to correspond to the desires or interests of the population and do not offer consistent and appealing solutions. The abstention rate (54 per cent) in the last general election (2022) mirrored this situation, as growing abstention undermines the legitimacy of the election as an expression of the will of the people. The National Assembly (parliament), which has become a mere echo chamber of power, the inept justice system and the anachronistic party system define the current Angolan institutional apparatus (Cedesa, 2023).

This overall situation – a little diffuse, where contradictory signs abound – leads to Angola being described as an anocracy. What is an anocracy? Anocracy has been defined as an unstable regime that combines elements of authoritarianism and democracy. An anocracy has incomplete mechanisms of dissent and consensualisation and is associated with permanent agitation or ungovernability, which hinders the political process (Gandhi and Vreeland, 2008). It is characterised by elections of some kind that take place, but these do not allegedly meet the high standards of competitiveness and fairness found in democratic systems (Mansfield and Snyder, 2007). Additionally, institutions in an anocratic regime that regulate the political process are relatively weak. As a result, instability and agitation tend to be the defining factors of anocratic regimes (Huntington, 1968). As Schipani (2010) pointed out:

> When discussing conflict proneness, much of the debate focuses on the democracy/autocracy dichotomy, while mixed regimes, or anocracies, are often an afterthought. This is unfortunate, given their prevalence, and more conflictual nature (relative to complete autocracies and democracies) (p. 1).

This characterises Angola today. There is a single party in power that controls the state and its main organs – namely, the judiciary, military, intelligence services and large state companies – while navigating within a formal democratic framework that is underdeveloped and underapplied. Nevertheless, the party allows a certain degree of dissent, a strong opposition and some free and critical press. However, the fact that people do not believe it is possible to remove the MPLA from power and that social and economic living conditions are worsening generates much unrest, with the country often resembling almost ungovernability. The last Afrobarometer survey about the quality of democracy in Angola assesses this aspect well, as three-quarters (75 per cent) of Angolans affirm that the country is going in the wrong direction and a majority of citizens describe their own living conditions (56 per cent) and the country's economic condition (68 per cent) as 'fairly bad' or 'very bad'. But, at the same time, they do not vote strongly for an alternative, presumably waiting for some miraculous new force to appear (Afrobarometer, 2024). It is not expected that, within the framework of a parliamentary discussion, it is possible to reach a consensus.

The 15+2 case (2015/2016)

In 2015, amid this general anocratic situation arose the 15+2 case. At the time, Angola was at the start of a long period of crisis and disillusionment (Verde, 2021). President dos Santos, who had held his position since 1979 and won the civil war in 2002 against Savimbi's UNITA, was watching an economic boom caused by a rise in oil prices turn into a bust due to unrestrained consumption and corruption.

With the economic crisis at hand, the government began to mobilise its forces to minimise the political effects of the slump. For example, it was reported that an army colonel had begun an extraordinary process of mobilising military personnel due to the economic impact of the crisis within the army. This colonel warned the soldiers that the country was in crisis but that they should not be alarmed by measures affecting the military. There would be austerity, for which we would have to be prepared, said the colonel during a graduation ceremony. Among the measures to be imposed on the military are salary cuts. 'Austerity will last for some time,' he emphasised. When speaking to the approximately 200 officers and soldiers present at the graduation, the colonel said that his unit had not carried out promotions the previous year 'because there was a drop in oil prices and promotions would create a lot of expense for the government'. In turn, a second speaker, the officer responsible for the brigade's patriotic education, asked the officers and soldiers 'not to be sad'. He appealed to the troops to 'remain calm', observe discipline and be courageous 'because the army does not go on strike' (Marques de Morais, 2015). This is an example of the challenges the government faced in 2015.

The public began to consider aloud that the elites had been living in an atmosphere of partying and easy money but, when faced with concrete reality and defiance, they had no solutions other than closing down the country and adopting several restrictive measures, be they in economic terms or regarding political overtures. Many measures were taken, only to make the situation worse. For example, banning imports only caused the internal market to be handed over to the two or three oligarchs that dominated it, creating inflationary pressure and eliminating competition. In the name of the crisis, a protectionist model based on patronage was legally implemented for the Angolan economy. It became patent to everyone that the easy economic model followed since 2002 was in disarray, most possibly beyond salvation. Discontentment rose (Verde, 2015b).

The context was challenging for political power. No fast solutions to the deep crisis were at hand. Enter the 15+2 case, mostly as a political distraction engendered by the Angolan Military Intelligence and Security Service (SISM). As referred to above, the SISM is the military branch of the security services, one of the three Angolan intelligence organisations. All of them worked under the direction of the President of the Republic and responded towards him.

The initial security service – Angolan Information and Security Directorate (DISA) – was created after independence. The structure and functional organisation of DISA was similar to that of the Intelligence and State Security bodies of the former socialist-bloc countries, whose principles were based on a single-party regime. DISA was an extremely powerful service and at that time could be considered one of the strongest among the Intelligence and Security Services of African countries. DISA was the only institution in Angola responsible for internal and external security, strategic information and special operations (Franco, 2013). It was later divided, but this initial genetic marker ended up defining the Angolan security service over time, despite the different names and historical and constitutional developments.

On the afternoon of 20 June 2015, 13 human-rights defenders and activists were arrested at gunpoint by the Angolan police while they were participating in a conference session on the ideological philosophy of peaceful revolution delivered by Domingos da Cruz in the Vila Alice neighbourhood of Luanda. The conference was based on Gene Sharp's book *From Dictatorship to Democracy* and was discussing peaceful methods of protest. Shortly after the arrests, police officers and members of the National Directorate of Criminal Investigation took the activists to their respective homes and seized their cameras and personal computers before eventually detaining them in a police jail.

Two days later, two more activists were detained. Authorities also filed formal charges against two female human-rights activists, Laurinda Gouveia and Rosa Conde, but did not detain them. Therefore, the group of activists became known as the Angola 15+2 (15 under arrest and 2 at liberty).

Among those detained were Domingos da Cruz, Luaty Beirão, Sedrick de Carvalho, Hitler Samussuku and Nuno Dala.[2] At the time, da Cruz was 31 years old and a university teacher. He had a degree in philosophy and a master's degree in legal sciences from the Federal University of Paraíba, Brazil and was the author of a book, *When War Is Urgent and Necessary*. Due to the book's title, in 2013, the Attorney General's Office of the Republic of Angola had accused him of committing the 'crime of incitement to collective disobedience', although the Luanda Provincial Court acquitted him, since the crime of which he was accused did not exist in Angolan legislation. Luaty was 33 years old and had degrees in electrical engineering from the University of Plymouth in England and economics and management from the University of Montpellier I in France. A musician and hip-hop artist, known in artistic circles as Ikonoclasta and Brigadeiro Mata-Frakuxz, he had been among those detained for an attempted demonstration on 7 March 2011, having announced it a week previously at a hip-hop show. The demonstration was inspired by the Arab Spring, which caused immense fear within the dos Santos regime. This was a first, as the demonstration demanded numbered resignation of José Eduardo dos Santos. Albeit the demonstrators numbered just 17 and nothing was happening, until some journalists came. That was when the police showed up and detained the demonstrators. They set up a large police apparatus to make an impression. The overreaction of the Angolan police to the 17 demonstrators can be explained, above all, by the fact that it was the time of the 'Arab Spring'. From December 2010 onwards, a wave of revolutionary demonstrations and protests took place in

[2] The full 15+2 group was composed of Domingos da Cruz, Sedrick de Carvalho, Luaty Beirão, José Gomes Hata, Nito Alves, Afonso Matias 'Mbanza Hamza', Hitler Samussuku, Inocêncio Brito 'Drux', Albano Bingo, Fernando Tomás 'Nicola', Nelson Dibango, Arante Kivuvu, Nuno Álvaro Dala, Benedito Jeremias and Osvaldo Caholo, who were detained in June 2015, plus Rosa Conde and Laurinda Gouveia, who were not detained.

the Middle East and North Africa. There were revolutions in Tunisia and Egypt and a civil war in Libya and Syria; there were also large protests in Algeria, Bahrain, Djibouti, Iraq, Jordan, Oman and Yemen and smaller protests in Kuwait, Lebanon, Mauritania, Morocco, Saudi Arabia, Sudan and Western Sahara. The protests shared civil-resistance techniques in sustained campaigns involving strikes, demonstrations, marches and rallies, as well as the use of social media, such as Facebook, Twitter and YouTube, to organise, communicate and raise awareness among the population and the international community in the face of attempts at repression and internet censorship by states. All of this could be replicated in Angola, the authorities apparently feared.

De Carvalho, aged 26, was a journalist in his fourth year of a law degree. He had started at the weekly *Folha 8* as a page editor in 2011 and later became a journalist. In 2013, he moved to *Novo Jornal*, covering society and economics, and in January 2015, he returned to *Folha 8*, again dealing with these areas. Samussuku, who was 25 years old and born in Moxico, was a fourth-year university student working on a political science degree. He was also a hip-hop artist belonging to the group Third Division, together with Cheik Hata. According to family members, Samussuku's father was a joker, which was why he chose the name Hitler, after the leader of Nazi Germany, for his firstborn, and Mussolini, after the Italian Fascist leader, for his youngest. Dala, aged 31, was a university teacher and researcher at the Technical University of Angola, as well as a teacher at the Centre for Care and Integration of Special Children. He had a degree in Portuguese from Universidade Agostinho Neto. In his text, entitled *Incitement to War or the Destruction of the Dictatorship?* Dala argued that the only path to structural change in Angola was through a non-violent process of popular revolution (Santos, 2015). Unlike the independence fighters, this group does not appear to follow any particular ideology, standing out for its proposals of non-violence, anti-dictatorship and the establishment of democracy. They are a reaction to a situation – the long prevalence of José Eduardo dos Santos and the MPLA – and did not represent anything more utopian or defined.

The Criminal Investigation Service of the Ministry of the Interior of Angola published a press release on the day of the arrests, announcing that 'various steps were taken that culminated in the arrest *in flagrante delicto* of 13 national citizens, who were preparing to carry out acts aimed at altering the country's public order and security' and that 'during the operation a series of pieces of evidence were seized' (Frontline defenders, s/d).

However, the detainees were not granted an arrest warrant, information about the reasons for their arrest or the possibility of contacting a lawyer or family (Carvalho, 2021). Only on 28 September 2015 were they notified of the content of the investigations conducted by the Attorney General of the Republic of Angola, which had been concluded, and that charges were being prepared. Meanwhile, Luaty Beirão had initiated a hunger strike on 21 September to protest against the arbitrary preventive detentions. The Angolan Constitution of 2010 does not contain any direct reference to the possibilities of pretrial detention; however, there has always been legislation permitting such detention, whose constitutionality has never been challenged. At the time, the pretrial detention regime was regulated by a statute of 1992, Law No. 18-A/92, of 17 July, and the truth was that the general rule of thumb allowed the usual application of this measure with no time limits being respected, despite there being a maximum period of 90 days under the terms of Article 25 of the aforementioned statute (Costa, 2015). In fact, this hunger strike was an important aspect that drew national and international public attention.

On 8 October 2015, the 15 defendants were finally formally charged with organising a coup d'état against President José Eduardo dos Santos and the government of Angola, as well as preparatory acts of rebellion. The two others who had not been detained, Conde and Gouveia, were also charged, having also participated in several meetings with the current inmates to discuss the principles of non-violent protest and political change in Angola.

The combination of Luaty Beirão's hunger strike and the absurd charges of conspiracy and rebellion led to an intense public reaction with national and international importance. It was clear to everyone that this group of young teachers, journalists and artists, without any weaponry, was not able to organise such a coup. How a group of 15 people without any weapons or relevant connections, whether with the police, armed forces or any armed group, could provoke a coup d'état or a rebellion that would threaten the current constitutional order, was never understood. There was a huge inconsistency between the accusations and the real factual possibilities. The idea sounded ridiculous.

At the national level, a Catholic mass was organised to express solidarity with the human-rights defenders detained in June and the deteriorating health of one of them, Luaty Beirão, who had been on hunger strike for 23 days. In addition, several interventions were made by activist websites, such as Rafael Marques' Maka Angola. Social media was the main point of dissemination of the incredulity and anger at the situation.

At the international level, the United Nations (UN) Special Rapporteur on the situation of human-rights defenders, Michel Forst, intervened, asking the government of Angola to release the activists. Frost mentioned that the 'deprivation of liberty on the sole ground of having promoted good governance and exercised the rights to free expression and peaceful assembly may be considered arbitrary', adding that 'such criticism is not only fully legitimate according to Angola's obligations under human rights law; it is also essential to the free and public debate necessary for a healthy civil society in the country' (UNHR, 2015, paras 2–3). Meanwhile, an association of lawyers from countries in the Southern African Development Community (SADC) announced their intention to monitor the trial. 'We are undoubtedly concerned about the case,' Makanatsa Makonese, executive director of the SADC Lawyers Association, told the Portuguese news agency Lusa, adding that two members of the organisation would monitor the trial of the Angolan activists in Luanda (Marques de Morais, 2015). In addition, the American Bar Association sent the famous lawyer Kimberley Motley to survey the case.

The trial itself was bizarre. It featured the judge exalting the virtues of President dos Santos and the prosecutor, ashamed of her role in the trial, hiding her face with long, false hair. The military intelligence service cantoned in a nearby room switched off the electricity in the courtroom when exchanges between the defendants' lawyers and the prosecution and judges became heated. One of the defendants, de Carvalho, referred to it as 'the clown court' (Carvalho, 2021, p. 115).

At the end of December 2015, it was crystal-clear that the trial would mark the beginning of the end of the regime's ability to control and detain without restraint. This trial brought to light a beleaguered and lost regime. The behaviour of the judge and the public prosecution were an example of the lack of independence of the judiciary, which clearly seemed to be simply following superior instructions. Faced with the legal ineptitude of dos Santos's officials, the trial went on absurdly, with interruptions and pauses oscillating between the arbitrary and the bizarre. One day, the activists' mothers say they will turn to the witch doctors to help them change the judge's evil spirit, who seemed bothered by such statements. The next day, the court's lights fail at a time when the exchange of words between the lawyers and the judge is intense. And in the end, the evidence about the so-called revolutionary conspiracy did not appear.

It was clear to the public that it had become impossible to defend the accusatory position, as no evidence of wrongdoing, beyond some speeches and readings, hardly considered indicators of a subversive movement, emerged.

The bulk of the evidence presented was the result of digital surveillance of the members of the 15+2 group. The regime made a point of showing the evidence obtained – without any known judicial mandate – both in court and on the TV and radio stations it controlled. The group's discussions were recorded using a ballpoint camera by two secret-service agents. The members of the group and their families were all subject to digital surveillance, before, during and after the trial. The location and capture of Domingos da Cruz was apparently carried out using mobile-phone tracking technology.

The evidence pointed to recording devices used being digital and included a video camcorder pen and a car-key fob device. Their small size allowed for surreptitious recording when compared to old-style analogue recording devices (for example, VHS cameras), which are too large for surreptitious recording.

In March 2016, the Luanda Provincial Court sentenced the 15+2 defendants to prison sentences ranging from two years and three months to eight years and six months for the alleged crimes of preparatory acts of rebellion and association with criminals, after the charges of organising a coup d'état against President dos Santos had been withdrawn by the prosecution. Based on the technicalities of criminal law, despite the fact that they were not considered to have attempted, much less committed, the crime, the court convicted them of mere preparation.

No one was convinced by the evidence presented or the farcical tone in which the trial took place, as the then general published opinion demonstrated (Verde, 2021). Furthermore, the evidence, which included videos digitally obtained illegally, had no legal force, as there was no warrant (Carvalho, 2021).

The case was seen as a diversionary strategy by the SISM, led by General Zé Maria, who was close to dos Santos, working with him since early days, occupying the function of Deputy Army Chief of Staff in 1991, and directing the military secret service since 2009. Zé Maria had ineptly tried to build a case that would divert attention from the declining economic situation and the president's leadership. This strategy was not successful, and the public reaction was vocal domestically and robust internationally. Susan de Oliveira wrote that it will always be clear that the trial was a grotesque farce from beginning to end. Amidst the masks and bad actors, the brave activists brought laughter and intelligent criticism from those who inevitably mark social transformations (Oliveira, 2016). Amnesty International considered the young people 'prisoners of conscience' and Human Rights Watch referred to the decision as ridiculous (Novo Jornal, 2016).

At the time, social networks and internet sites were already replacing the traditional press. Mastery of the public space was no longer possible, therefore the public outcry, regarding the trial, was everywhere and government did not have the means to control the digital world.

The image of progress and growing democracy that the government had been trying to present over the years was collapsing, exemplified, for example, by the approach with CNN International since 2012 where the government provided the news agency with funding to promote a positive image of Angola around the world (Maka Angola, 2012). Therefore, the government raced to fix the blunder.

The decision of the court of first instance was always subject to appeal to the Supreme Court. And so it was done. At the end of June 2016, the Supreme Court, in a terse decision against the trial judge, ordered the release of the defendants. Sedrick de Carvalho argued that this was the first step of 'cleaning up the government' by criticising the trial judge. By then, all the errors and wrongdoings of the process had become his fault. The Supreme Court ordered the initiation of disciplinary proceedings against the trial judge by the Judicial Council (Carvalho, 2021, pp. 185–6). Today, we know that this was cosmetic, as in 2019, the judge was promoted to the Court of Appeal.

However, the matter did not end there. On 20 July 2016, an amnesty law was approved that ended the proceedings against all the defendants. Albeit, released by a Supreme Court decision, such court order referred to the provisional detention or 'pre-trial detention'. The group had to serve a prison sentence in the future. With the amnesty law everything was gone. The process was erased.

It is curious that the same law also exempted most of the economic crimes that could be attributed to the regime's top leaders in the future.

What remains of this case are aspects that are relevant to the analysis we intend to carry out on the role of security and intelligence services, the use of digital surveillance and the possible role of public opinion and mobilisation.

First, it has now been proven, by the constant presence of its members during the trial and the digital vigilance material presented in court, that the operation was planned by the SISM and its head at the time, General Zé Maria, to alleviate the pressure on the government due to the economic decline (Verde, 2021).

Second, SISM had at its disposal all the police and judicial resources in the country, controlled the trial by being conspicuously present and were also responsible for several videos of 15+2 meetings shown as essential evidence. Regarding the illegal surveillance, Samussuku noted that the security services managed to infiltrate the meetings with at least two young people and used surveillance cameras throughout the debate sessions in which the 15+2 participated in Vila Alice (Interview, Hitler Samassuku, 2023). In fact, there is no judicial record of the way and means by which these videos were obtained and no reference to any court order as legislation obliged or otherwise. Nevertheless, they were not declared null or void by the judge in the case.

Third, the response from the public was decisive, with lawyers from the American Bar Association, for example, international organisations (UN, Amnesty International, Human Rights Watch and press and social media (Público, DW, Maka Angola)) paramount in creating an awkward environment for the government. As Domingos da Cruz, a defendant in the case, related to this book, civil society's response had two phases. Initially, there was shock and fear. The case paralysed people, and many citizens believed the narrative of a group organised to carry out a coup d'état constructed by the regime, based on videos captured through surveillance and shown by the media constantly. In the second phase disbelief was born, and the public began to question the veracity of the videos and the legality of the actions that captured them, thanks to the efforts of lawyers to educate the public about the law and the significant contributions of the free press inside and outside the country, made through social networks (Interview, Domingos da Cruz, 2023). Samussuku said that this was a timely, necessary and urgent response, arguing that after a few days friends of the defendants started sharing the defendants' profiles on social media, which led to a wave of solidarity in the social media and public conversations in meeting places such as coffee shops, bars and so on. If it were not for this, the defendants might have been killed, with the security services presenting a manufactured version of their deaths to the public, as had happened in the past. When the public learnt that they were artists, students and young people who were civic leaders in their communities, they decided to raise their voices with the slogan 'freedom now' (Interview Samussuku, 2023).

Public reaction as a watershed in the 15+2 case

As seen, the 15+2 case brought about defeat for the Angolan government of dos Santos, leading to a retreat that ultimately resulted in a new amnesty law that sought to definitively put an end to the issue. Nevertheless, in the end this defeat contributed to the delegitimisation of the dos Santos regime and, most probably, in part, to his decision to withdraw from the presidential election in 2017. Teixeira Cândido, the leader of the only journalists' union existing in Angola, said that the government had backed down owing to public pressure, both national and international. It was an active reaction that exposed the arbitrariness of the government and judicial bodies (Interview, Teixeira Cândido, 2023). Rafael Marques, a well-known human-rights activist, described the case as blatant incompetence. The arrest of the 15+2 never made any sense, and everything else was a race to the abyss (Interview, Rafael Marques, 2023). Media coverage and internal and international pressure exposed too many errors, which made a retreat possible, suggested the lawyer Margarida Nangacovie, meaning that given the errors exposed, there was no other option but withdrawal (Interview, Margarida Nangacovie, 2024). In fact, it quickly became clear that the evidence had not been collected in accordance with criminal rules, and even that which was presented in court did not reveal any dangerous conspiracy, only meetings to discuss theoretical non-violent ways of changing the regime. There were no plans to occupy palaces, recruit security forces, arm them; nothing.

Clarice Vieira, a law teacher, believed that the government backed down due to international pressure because it needed to show the international community that democracy existed in Angola and because civil society had made so much noise (Interview, Clarice Vieira, 2023). The same was said by the journalist Eliseu Ngola (Interview, Eliseu Ngola, 2023). Filomena Azevedo, a businesswoman with public influence, emphasised that the government had relented because there was much anger about this case (Interview, Filomena Azevedo, 2024).

The causes of the resolution of the 15+2 process are unanimously accepted. It was a successful case of public pressure that limited the effects of political persecution based, among other things, on illegal digital surveillance, with the pressure applied both nationally and internationally.

However, no one has highlighted which specific sources of pressure were useful and which were not. There was a feeling transversal to the government authorities and civil society of global pressure, but what had this translated into? It is a fact that there were no street demonstrations, general strikes, or non-violent combat by the population (even less, violent combat). Added to this was the fact that the press, TV and radio were essentially controlled by the government. What we might call the classic media – television, radio, printed newspapers – whether state-owned or privately owned – were aligned with the government, with one or two irrelevant exceptions. Therefore, it was not from the street or from classical media outlets that this public outrage was translated.

We can point out three axes of embarrassment that departed from the classic forms as street protest and use of traditional media. The first resulted from the widespread media coverage of Luaty Beirão's 36-day hunger strike. Probably because he was Portuguese-Angolan and the son of one of the symbols of the dos Santos regime, José Beirão, who was general director of the José Eduardo dos Santos Foundation until his death in 2006, Luaty Beirão received widespread interest from the Portuguese press. From there, the interest spread out to the world. Apparently, the Portuguese media projected Luaty Beirão and his hunger strike. He confessed:

> I was completely astonished by the almost pornographic level that this thing [hunger strike] took. All that was left was for the Vatican to speak out. It reached the United Nations, the Department of State of the Obama Government. It reached a point such that there was nothing left to do, except for the [Angolan] Government to give in (Lusa, 2016).

It is interesting to note that the closer he was to death, the more the issue gained international importance, almost demonstrating that the existence of martyrs is necessary for the international community to take human-rights issues seriously. Beirão admitted that on the 19th day of the hunger strike, he had begun to fear for his life but that the Angolan government had started to take the protest more seriously (Lusa, 2016). The adverse publicity from the Portuguese press was one of the reasons for the Angolan government to take the case seriously. That suggests a very colonial mindset, still predominant in Angolan elites, who developed most of their educational, recreational and business activities in Portugal.

A second axis was the use of social media, mostly news portals and Facebook posts. The Angolan government was used to controlling the media, with direct or indirect ownership of television and radio stations and newspapers. Any dissent generally ended with the million-dollar purchase of the medium in question for later closure, as happened, for example, with Semanário Angolense of Graça Campos.

Although social media already existed, it was not yet widespread or, at least, the intelligence services were not fully qualified to deal with it. Therefore, all the discontent was channelled through websites and Facebook. It was on these platforms that the main fight took place – in terms of legal arguments against the case (Maka Angola) and, humorously, the prosecutor's hair (Facebook). It was a time of digital effervescence that caught the old generals off guard.

Finally, there was international pressure. The US State Department, the United Nations and the American Bar Association have already been mentioned. Even an attorney from the Portuguese Public Prosecutor's Office and member of the national board of the Prosecutors' Union of Portugal wrote a column in a Portuguese newspaper stating that the most basic procedural guarantees of defence of the accused had been grossly trampled on in Angola (Sousa, 2016).

As will be seen later, it was a moment of singularity with a set of circumstances almost unrepeatable in an anocratic regime – or at least not predictable. It could happen at any time, or it could happen never again. In the end, it was difficult to create from this case a broad and general applicable rule regarding public oversight.

Legal framework: From text to factuality

Formally, the Constitution of the Republic of Angola is clear regarding the protection of the right to privacy, prohibiting digital surveillance unless there is a judicial warrant. Article 34 clearly and eloquently establishes that '. . . the confidentiality of correspondence and communications, regardless of the means used, cannot be subject to surveillance of any kind. If necessary, surveillance can only occur with judicial authorization' (Constitution of the republic of Angola, 2010).

Angolan legislation addresses communications and social information services in the country, regulating these and the provision of digital content. It is worth mentioning that, although the Constitution protects against digital surveillance, requiring judicial authorisation, other laws may present contradictions or ambiguities in relation to this topic. In Angola, specific laws related to digital surveillance are deemed fundamental to protecting citizens' rights in the digital environment. Although the Constitution of the Republic of Angola establishes general principles, other specific legislation also addresses privacy and surveillance issues. Listed below are some of them:

Personal Data Protection Law: Law No. 22/11 of 17 June regulates the processing of personal data in Angola. It establishes the rights of data subjects and the obligations of those responsible for processing that data. This law aims to protect citizens' privacy and restrict the misuse of personal information.

Electronic Communications Law: Law No. 23/11 of May 20 deals with electronic communications, including the surveillance of telecommunication networks. It establishes rules for the interception of communications, ensuring that surveillance occurs only with legal authorisation.

The above statutory laws were in force when the 15+2 case occurred, although they, as well as Article 34 of the Constitution, were not even considered in the case. Therefore, the surveillance occurred outside the framework of these laws.

The fact is that until 2011 Angola did not have a personal data protection law; therefore, a culture of non-legality was pervasive. That year, Law No. 22/11 of 17 June was approved and with it a data protection agency was created. Under Article 44, this agency was composed of seven citizens, three of whom were designated by the president of the republic, three by the National Assembly and one was elected by the Superior Council of the Judiciary. The supervision of digital surveillance and data intelligence was, therefore, carried out by a data protection agency that, under the terms of the law, belonged to the interdependent State Administration and maintained a cooperative relationship with the Executive – in this case, the president of the republic – under the terms of Articles 69 and 120, in fine, of the Constitution.

Related to the intelligence services, the law in force at the time was enacted in 2002 (National Security Act). This Act required the intervention of a Supreme Court judge to authorise any interception of communications.

Therefore, from a positive point of view, the law in Angola is sufficiently robust and comprehensive. Since 2011, the country has built a methodical legal framework regarding digital surveillance out of almost nothing.

However, reality is very different from the law. João Pinto, an unexpected source, as he is a former Member of Parliament for the MPLA, a Deputy Whip of the parliamentary party and now Inspector General of the state, asserted that the degree of independence of the above-mentioned Data Protection Agency is fragile, as there is broad discretion in the appointment of its members by the three state powers. Therefore, the nominees of the Data Protection Agency are conditioned for reasons of lack of patrimonial, administrative and functional autonomy. The principles of nonremovability and stability of its members do not have practical application since the presidential decree that approved the Statute of the Data Protection Agency allowed for the discretionary appointment and dismissal of members appointed by the president of the republic (Interview, João Pinto, 2023). Samussuku, a defendant in the 15+2 case, went further, emphasising that the fact that Angola was an excessively centralised state, where political power was in its entirety confined to the MPLA, should be considered. Consequently, it was not possible to ascribe any independence to the so-called independent entities, because the leaders previously responsible for these bodies were politically active in the party, which was confused with the state. From this logic, defending the party was understood as defending the state. If the MPLA wanted any surveillance information about someone, these bodies were not able to reject it (Interview, Hitler Samussuku, 2023). The same evaluation was made by Eliseu Gonçalves, a former aide to President dos Santos, who reflected that it was important to highlight that the ruling party, the MPLA, had almost complete control over regulatory bodies. For example, the Ministry of Telecommunications, Information Technologies and Social Communication was responsible for supervising the technology sector, while Angolan Institute for Communications (INACOM) served as the sector's regulatory body. INACOM determined the sector's regulations and policies, set prices for telecommunication services and issued licences (Interview, Eliseu Gonçalves, 2023). This mean that any intelligence oversight from public/state powers is always conditional and submitted to political constraints.

It can be concluded that the legal text in Angola is less important than practice. Rosianne Pávla, a lawyer, explained that there was a legal framework that was robust but also ineffective due to the political interference in the institutions that dealt with the matter (Interview, Rosianne Pávla, 2024).

This reality is the result of the existence of a party, the MPLA, whose own history is intertwined with the Angolan state, as it has always been in power, both in dictatorship and democracy. Thus, there is no prospect of democratic alternation, which leads all decision makers, independent or not, to adopt behaviours compatible with the MPLA's permanence in power. This reminds us of the model advanced by Ramseyer (1994):

> Players who expect to play [any player considered in the game theory] indefinitely may sometimes defect and sometimes cooperate. So too with whether rational politicians keep courts independent. Fundamentally, whether they keep them independent (whether they adopt the cooperative strategy) depends on two things: (a) whether they expect elections to continue indefinitely and (b) if elections will continue, whether

> they expect to continue to win them indefinitely. Only where they rate (i) the likelihood of continued electoral government high, and (ii) the likelihood of their continued victory low might they provide independent courts (p. 722).

This fits Angola perfectly. Although it is expected that elected government will prevail, it is also anticipated that MPLA will win every time; therefore, there does not exist any incentive to create de facto independent courts or supervisory organs. The absence of a viable political alternative is a factor too. It seems like disaffection is translating into declining voter participation rather than support for an electoral alternative, which is to the advantage of MPLA. This is a global trend – this means, disengagement from formal politics especially among the youth, which makes it more necessary that public oversight is encouraged as the formal institutions tied to electoral politics are representing fewer and fewer people. That is an important trend across the board.

The essential conclusion that comes from a legal analysis is the opposite of a legal analysis; rather, it is a factual or political analysis. The common perception is that there are no independent adjudicators in Angola, whether they be courts or autonomous administrative entities. The consequence is that it becomes difficult in such an environment to apply the law. The problem is not with the law but with the environment and with enforcement. It is important to note that there is a school of thinking in law, critical legal scholarship, which considers the law to be inherently political and looks at how law is designed to look good but be unimplementable in reality and restrained by social and political structures. Positivist legal theory would look at the legal instruments only and not at the conditions in which they are developed and implemented, which does not explain the situation in Angola (Kairys, 1998).

Colonial roots: A surveillance culture that prevails

The entrepreneur Filomena Azevedo was adamant in saying that, in Angola, colonialism affected everything: ‘Almost everything we do here is similar to the Portuguese' (Interview, Filomena Azevedo, 2023). This evaluation of the culture of surveillance that exists in Angola is almost unanimous. The roots of a paramount culture of unhindered surveillance are found in colonial practices. Rafael Marques, a well-known human rights activist, went somewhat further, adding the impact of Marxism-Leninism and a melting pot of intelligence and surveillance practices that the old regime collected from various parts of the world.

Until recently, the Angolan penal code was that of Imperial Portugal from 1886, which did not contain relevant safeguards concerning surveillance and none regarding digital surveillance. Therefore, the colonial impact on the creation and application of laws was clear (Interview, Rafael Marques, 2023). The same approach was purposed by Samussuku, who stated that the MPLA followed, to the millimetre, the colonists' codes of domination and surveillance against the people they said they had freed from the colonial yoke. The MPLA inherited the practices of the Portuguese political police and then combined them with the Cuban experience of surveillance against everything and everyone, including some of its militants who presented positions that were at times not in line with the president (Interview, Samussuku, 2023). MPLA, despite being a liberation movement, or because of that, never adopted a vision for the democratic development of the country. Perhaps the civil war hindered any efforts as the support of the Soviet Union implied some kind of communist regime. That meant that MPLA had no emancipatory vision for intelligence and transformation programme post independence.

The reality is that there is a convergence of two authoritarian forces in the definition of the Angolan security services' attitudes and behaviours.

The first force, which could be designated as structural-cultural, is derived precisely from colonial practices. The Angolan PIDE (Secret Portuguese Police) delegation was formally established in Angolan territory in 1954, but its presence was residual. From 1961 onwards, with the outbreak of armed conflict in the territory, control measures increased with the multiplication of delegations, subdelegations and posts in various districts of the territory, and with the creation of the Angolan Centralization and Coordination of Information Services (SCCIA), which complemented the PIDE's 'empirical research' with the centralisation and processing of information, studies, statistics and reports, forwarded from lower levels. This institutional multiplication, responding to the emerging conflict situation, implied a substantial expansion of the information production network (namely through the network of informants), as well as the creation of paramilitary forces (*Os Flechas*). A strong apparatus covering border control, infiltration into independence groups, counterespionage, social observation and military support, was created (Blanes, 2013). The objective was to persecute nationalists and, to this end, the force had a vast system of prisons and work camps, which were nothing more than concentration camps, such as São Nicolau in Angola, where nationalist guerrillas were taken, mixed with populations displaced by the conflict. In these camps there were prisons, work zones and even satellite villages. The conditions were inhumane, with cells measuring 20 metres by 40 metres containing 200 people, and cases of rape and various types of torture, such as the burial of people alive, crucifixions and shootings. The police were the result of a regime of totalitarian influence, albeit with a great paternalistic nature, that served as an example for other countries, including Brazil, with the Estado Novo under the control of Vargas. The PIDE was used to repress any act that meant a change in the political, social, economic, cultural or religious status quo in the Portuguese colonial empire (Mendonça, 2018). It was a body strongly operationalised in the culture of surveillance and control. Taking this into consideration, it can be said that it influenced how the Angolan state operationalises today, reacts to issues of (in) security and, in relation to these, considers its protagonists, according to Margarida Nangacovie (Interview, Margarida Nangacovie, 2024).

However, it is necessary to broaden the approach and mention that colonial influence is not seen only in terms of the powers and functions of the political police because it has structural characteristics. Simply looking at the legislative history that leads us to the present, the various constitutional moments that followed after independence broadly corresponded to a legal structure influenced by colonialist practices, where authoritarianism and centralisation were predominant, and did not coincide with what was known from pre-colonial history but rather with the functional aspects of colonial power. What happened after independence was that such a structure was dressed according to different ideologies – that is, Marxist until the 1990s and then liberal democratic. However, it maintained the substance of the powers and mechanisms of the colonising state. Simply put, the colonial Portuguese structure of centralised and unsupervised power, just dependent on the President of the Council of Ministers, Oliveira Salazar, without any real oversight became the basic latent matrix of Angolan constitutionalism (Verde, 2025).

Obviously, the Soviet-Cuban influence should also be considered, as it reinforces the colonial one, as Marques and Samussuku highlighted. Nevertheless, this influence can be characterised as operational rather than structural. Agostinho (2018) described a first phase regarding the establishment of security services in post-independence Angola (1975–91), in which it was feasible to build a state with a Marxist matrix that was non-democratic and with a single-party system, where there was a monopoly and the predominance of state power over society, privileging defence and security structures over other ones, due to the revolutionary period and regional upheavals occurring in the historical moment, as well as the post-independence civil war. In this context, an intelligence service with a Soviet matrix was built.

The construction of this intelligence system took place in 1975, as mentioned above, with the approval of Law No. 3/75 of 29 November, 1977 which created the DISA. The DISA emerged because of the period of unrest subsequent to the declaration of independence in 1975, so the structuring process, as well as its attributions, was influenced by the non-democratic political regime in force at the time in Angola. The DISA had procedural powers; that is, it conducted investigations, instructed proceedings and finally referred cases to the courts or police bodies, depending on the case. In practice, the DISA acted as the Public Prosecutor’s Office. That was not enough, and the DISA's powers were increased by Law No. 4/77 of 25 February 1977 on the Prevention and Repression of the Crime of Mercenaryism and by Law 7/78 of 26 May 1978 on Crimes Against State Security, which not only densified procedural powers but also strengthened the non-democratic regime with repressive bodies and a partisan police force. The security-service structure had areas that carried out secret operational investigation activities, criminal and operational investigations, procedural instruction, trials and criminal re-education. These activities were identical to those of an overall police body fundamentally directed against actions opposing the non-democratic regime (Agostinho, 2018).

It is not within the scope of this work to carry out a comparative intelligence and security exercise. What is important to mention is that a totalitarian perspective of surveillance and general control promoted by both colonial and Marxist practices decisively influenced the ethos of the security services in Angola and their relationship with the population and vice versa.

It is evident that since the 1970s and 1980s, there have been several changes in the Angolan intelligence services as well as new operational influences, such as Mossad, which contributed with training and advanced technology and an adaptation to the democratic constitutionalism of 1991/1992 and then in 2010 (the present Constitution). Today, there are three services, one for external intelligence, another for internal security and a third for military information, in a model similar to that adopted by democratic Portugal, as well as a separation between police and prosecutorial services.

However, what can be seen from various interviews is that the idea of an all-powerful secret service persists exactly as in the past. For example, Teixeira Cândido had no doubts that the state had been investing heavily in surveillance, using Chinese, Israeli, Russian and American technologies. People had no way of opposing the state's means. Journalists took courses to prevent this, but the resources invested were disproportionate (Interview, Teixeira Cândido, 2023).

Changes after the 15+2 case: Just an illusion

Logic would lead us to think that the 15+2 case had a significant impact on Angola, especially with regard to human rights and freedom of expression. The case attracted national and international attention to the situation of the political activists in Angola. Many people showed solidarity with the detained activists, demanding justice and freedom for them. The arrest of the 15+2 activists demonstrated the Angolan Government's repression of freedom of expression and dissent. This created an environment of fear and inhibited the free expression of critical opinions. International human-rights organisations, such as Amnesty International, closely followed the case. International pressure contributed to the release of the activists from prison and their transfer to house arrest. The 15+2 case led to discussions about the need for legal and political reforms in Angola.

In summary, the 15+2 case highlighted the vulnerabilities faced by political activists in Angola and encouraged debates about freedom of expression and justice in the country. The 15+2 case seemed like a watershed moment, although it was not. The strength of public opinion, both nationally and internationally, forced an authoritarian government to retreat completely. It was expected that, from then on, the courts would be more careful, the intelligence services would follow the law more proficiently and, in general, there would be more intervention by the public.

In fact, as seen, the advent of João Lourenço as President of the Republic (2017) inaugurated a legislative effort aimed at regulating a series of practices that were not foreseen in the law as well as creating a new penal and criminal procedure code.

However, the perceptions gained in the field study carried out for this work in 2023/2024 do not support this logic. It appears that the 15+2 case was an exception that confirmed the rule of the non-accountability of electronic surveillance and the actions of the intelligence services.

Domingos da Cruz, one of the 15+2 and presently a researcher at a Spanish university, was adamant, saying that, as far as he knew, no change had taken place, either legally or in practice. As for civil society, there had been no systematic, high-quality or consistent actions, just mere fragments of actions. Angolan civil society was poor, resulting from the general low-level development of the country and fragility enhanced by all the obstacles imposed on it by the regime, with active collaboration from the international community to keep the country as it is and under the control of the MPLA (Interview, Domingos da Cruz, 2023). The same assessment was made by Samussuku, another of the 15+2, who stated that the regime was the same, did the same things and continually made the same mistakes (Interview, Hitler Samussuku, 2023). Clarice Vieira, a lawyer, did not disagree. She stated that there had been no changes in supervision practices in light of controversies concerning digital surveillance or opportunities for responses and proactivity from civil society or journalists. Abuses and arbitrariness were still committed within the scope of digital surveillance, including towards the exercise of freedom of expression and of the press, which were repressed in different ways, and all information was controlled and delimited. In short, everything was controlled, and there was a very special democracy in Angola with its own characteristics (Interview, Clarice Vieira, 2023). Filomena Azevedo, a businesswoman with strong intervention in the public space, did not disagree and asserted that there had been no change. Journalists were increasingly taking a stand, but they still feared the 'system', which was why they did not do it any more. Civil society would arrive with much strength and then end up giving up (Interview, Filomena Azevedo, 2023). In addition, Teixeira Cândido revealed that there had been no changes in surveillance practices; rather, there was more sophistication in surveillance methods (Interview, Teixeira Cândido, 2023). In fact, the promised advances have not materialised.

The perils of an anocratic regime

An anocratic regime is defined by oscillation and uncertainty (Regan and Bell, 2010). It is neither a democracy nor a dictatorship, but has elements of both. It allows dissent, but the limits are not known. It has mechanisms of freedom, but the borders are not known. The state is powerful and does not act under the rule of law, but sometimes it does.

Indefiniteness and uncertainty characterise this regime, which becomes prone to unrest. Due to these characteristics, it does not allow for a consistent model of the supervision of digital surveillance by public opinion.

In fact, it sounds as if international pressure, culminating in the embarrassing spotlight put on the hunger strike by the Portuguese press, tilted the case towards the defendants. Internally there was limited follow-through by the state and even by activists as the groundswell was not sufficiently locally rooted. The international campaign work did not seem to build local capacity. Perhaps, international actors should have maintained constant pressure and tried to work in conjunction with local groups.

What the 15+2 case demonstrates is that, in certain circumstances, translated into obvious injustice, the physical and moral courage of activists, widespread outrage on social media and strong international institutional pressure and, public opinion can reverse the arbitrary positions of an anocratic regime. However, this does not create a permanent trend or structure; it is case by case. In this specific case, it seems that the emergence of a possible 'martyr', intense external pressure and the work of social networks were sufficient elements. However, this conclusion leaves the question: does it take a 'martyr', deaths or near deaths for public pressure to be effective in curbing the abuses of digital surveillance?

In the end, the 15+2 group disbanded. Some continued their activism (Luaty Beirão), others joined UNITA, the main opposition party (Hitler Samussuku and Nuno Álvaro Dala, the latter of whom is now a Member of Parliament). Sedrick de Carvalho is a book publisher and Domingos da Cruz has furthered his academic career. Others have disappeared from the public sphere. The truth is that they no longer function as a group.

References

Afrobarometer. 2024. Angolans' approval of their president on the decline, say country is going in the wrong direction, new Afrobarometer study shows. *Afrobarometer*. [Online]. Available from: https://www.afrobarometer.org/articles/angolans-approval-of-their-president-on-the-decline-say-country-is-going-in-the-wrong-direction-new-afrobarometer-study-shows/. Accessed on 20-10-25 last time.

Agostinho, E. 2018. *Os serviços de inteligência e segurança do Estado face a Constituição Angolana*. Lisboa: Repositório Institucional da Universidade Autónoma de Lisboa.

Bacelar Gouveia, J. 2014. *Direito Constitucional de Angola*. Lisboa: IDILP.

Blanes, R. 2013. Da confusão à ironia. Expectativas e legados da pide em Angola. *Análise Social*. 206, xlviii (1.º).

Cedesa. 2023. *Angola. Nova Constituição, Nova República*. [Online]. [Accessed 25 April 2024]. Available from: https://www.cedesa.pt/2023/01/30/angola-nova-constituicao-nova-republica/.

Costa, D. 2015. *A prisão preventiva em angola e perspectivas de evolução do seu regime jurídico*. Coimbra: Faculdade Direito Coimbra.

Cruz, D. 2021. Angola: Vigilância digital e necropolítica. *Observatório da Imprensa*. [Online]. Available from: https://observatoriodaimprensa.net/angola-vigilancia-digital-e-necropolitica/. Accessed 20-10-25-Last time.

De Carvalho, S. 2021. *Prisão política*. Luanda: Elivulu.

Franco, M. 2013. *A evolução do conceito estratégico do serviço de inteligência e de segurança do estado da república de Angola (1975–2010)*, ISCSP, Lisboa.

Front Line Defenders. n/d. *Histórico do caso: angola 15+2*. [Online]. [Accessed 1 March 2024]. Available from: https://www.frontlinedefenders.org/pt/case/case-history-angola-15.

Gandhi, J. and Vreeland, J. 2008. Political institutions and civil war: Unpacking anocracy. *Journal of Conflict Solutions*. 52(3), pp. 401–25. [Online]. Available from: https://pordentrodaafrica.com/noticias/a-sentenca-final-dos-152-o-suplicio-e-o-riso-manter-se-humano-frente-ao-que-desumaniza.

Huntington, S. 1968. *Political order in changing society*. New Haven: Yale University Press.

Kairys, D. 1998. *The Politics of Law*. New York: Basic Books.

Lusa. 2015. Advogados da SADC em Luanda para o julgamento dos 15+2. *Maka Angola*. [Online]. [Accessed 4 March 2024]. Available from: https://www.makaangola.org/2015/11/advogados-da-sadc-em-luanda-para-o-julgamento-dos-152/.

Lusa. 2016. Luaty Beirão 'estupefacto' com uma greve fome que deu a volta ao mundo. *Observador*. [Online]. [Accessed 10 February 2024]. Available from: https://observador.pt/2016/10/17/luaty-beirao-estupefacto-com-uma-greve-fome-que-deu-a-volta-ao-mundo/.

Maka Angola. 2012. CNN Planeia Cobertura Favorável de Angola. *Maka Angola*. [Online]. Available from: https://www.makaangola.org/2012/02/cnn-planeia-cobertura-favoravel-de-angola/. Accessed 20-10-25-Last time.

Mansfield, E. and Snyder, J. 2007. *Electing to fight: Why emerging democracies go to war*. Cambridge: MIT Press.

Marques, A. 2013. *Segredos da Descolonização de Angola.* Alfragide: Dom Quixote.

Marques de Morais, R. 2015. Exército mobiliza tropas para enfrentar a crise económica. *Maka Angola.* [Online]. [Accessed 13 March 2024]. Available from: https://www.makaangola.org/2015/01/exercito-mobiliza-tropas-para-enfrentar-a-crise-economica/.

Mendonça, A. 2018. O Salazarismo e a PIDE: política de repressão em Angola. *Faces da História*, Assis-SP. 5(2), pp. 297–315.

Novo Jornal. 2016. Caso 15+2. Às pesadas condenações seguem-se os recursos e a pressão internacional sobre o Estado Angolano. *Novo Jornal.* [Online]. Available from: https://novojornal.co.ao/sociedade/interior/caso-152-as-pesadas-condenacoes-seguem-se-os-recursos-e-a-pressao-internacional-sobre-o-estado-angolano-37.html. Accessed 20-10-25- Last time.

Oliveira, S. 2016. A sentença final dos 15+2: O suplício e o riso. Por dentro da África. https://pordentrodaafrica.com/noticias/a-sentenca-final-dos-152-o-suplicio-e-o-riso-manter-se-humano-frente-ao-que-desumaniza

Oliveira Pinto, A. 2015. *História de Angola. Da Pré-História ao Início do século XXI.* Lisboa: Mercado das letras. https://pordentrodaafrica.com/noticias/a-sentenca-final-dos-152-o-suplicio-e-o-riso-manter-se-humano-frente-ao-que-desumaniza

Ramseyer, J.M. 1994. The puzzling (in)dependence of courts: A comparative approach. *The Journal of Legal Studies*. 23(2), pp. 721–47.

Regan, P. and Bell, S. 2010. Changing lanes or stuck in the middle: Why are anocracies more prone to civil wars? *Political Science Quarterly*. 63(4), pp. 747–59.

Santos, C. 2015. Quem são os ativistas presos desde 20 de junho e as acusadas que não estão detidas? *Esquerda*. [Online]. [Accessed 22 April 2024]. Available from: https://www.esquerda.net/dossier/quem-sao-os-ativistas-presos-desde-20-de-junho-e-acusadas-que-nao-estao-detidas/39200.

Schipani, M. 2010. *Regime completeness and conflict: A closer look at anocratic political systems.* PhD thesis, Georgia State University.

Soares de Oliveira, R. 2015. *Magnificent and beggar land. Angola since the civil war.* London: Hurst.

Sousa, R. 2016 Angola: O caso 15+2. *Público.* [Online]. [Accessed 15 March 2024]. Available from: https://www.publico.pt/2016/04/13/mundo/opiniao/angola-o-caso-152-1728860.

UNHR. 2015. UN expert urges Angola to release fourteen rights activists detained for criticizing the Government. [Online]. [Accessed 14 February 2024]. Available from: https://www.ohchr.org/en/press-releases/2015/10/un-expert-urges-angola-release-fourteen-rights-activists-detained.

Verde, R. 2015b. Perplexidades acerca da presente crise económica angolana. *Maka Angola.* [Online]. [Accessed 12 February 2024]. Available from: https://www.makaangola.org/2015/02/perplexidades-acerca-da-presente-crise-economica-angolana/.

Verde, R. 2021. *Angola at the crossroads. Between kleptocracy and development.* London: I.B. Tauris.

Verde, R. 2025. Direito Constitucional de Angola. História, Constituições e Teoria da Constituição. Ufolo, Luanda.

CHAPTER THREE

Popular agency oversight of digital surveillance of communications and personal data for intelligence purposes: The case of Botswana

Tachilisa Badala Balule

Introduction

This chapter interrogates popular agency oversight of digital communications and personal data over the intelligence sector in Botswana. The term popular agency oversight in this chapter refers to public involvement through civil society organisations (CSOs) and the media in the oversight of the intelligence sector. CSOs are the sphere of voluntary collective actions by citizens that develop around shared interests, purposes and values (Cole et al., 2008, p. 14). Popular agency oversight allows the public and CSOs acting on their behalf to scrutinise and monitor actions and decisions of intelligence agencies to ensure responsible use of power and accountability. Popular agency oversight is distinguished from traditional formal oversight mechanisms over the intelligence sector through arms of government such as the executive, legislature and judiciary. Intelligence services play a key role in ensuring the security and stability of a state by preventing internal and external threats to the state. Many of the threats to the security of a state are often covertly organised, and intelligence services need intelligence to counter such threats. This may call for intelligence services to resort to covert means to prevent threats to the security of the state. Some of the methods used by intelligence services in countering threats to the security of the state are intrusive and may infringe upon human rights. The apparent tension between the protection of human rights and the security of the state has led to a view that the two interests are diametrically opposed. Burke-White (2004, p. 249) argues that US foreign policymakers tended to view the promotion of human rights and the protection of national security as mutually exclusive. He notes that the approach has been either to promote human rights at the expense of national security or protect national security while overlooking human rights. The House of Lords has, however, observed that, although there may appear to be a tension between the protection of the security of a state and civil liberties, the two are on the same side. The court further observed that '. . . in accepting as we must, that to some extent, the needs of national security must displace civil liberties, albeit to the least possible extent, it is not irrelevant to remember that the maintenance of national security underpins and is the foundation of all our civil liberties' (*R v Secretary of State ex parte Cheblak,* 1992, p. 334).

What the House of Lords is saying is that the security of a state is worthy of protection in a derivative sense, because of its purported necessity for the well-being of its citizens. Covert means, especially those that intrude on human rights, must only be used where there is a pressing social need for their use, justified by an overriding public interest. Accountability of intelligence services in how they conduct their business becomes important to ensure that they do not unjustifiably infringe upon civil liberties.

Accountability is one of the hallmarks of a democracy. The expectation that government in a democratic state will be answerable to the people is a necessary condition for recognising a state as democratic and is also accepted as a standard for political legitimacy (Borowiak, 2011, pp. 6–9). Parsons and Molnar (2018, pp. 144–54) argue that 'accountability exists when there is a relationship where an individual or institution, are subject to another's oversight, direction or request that the individual or institution provide information of justification for its actions'. Accountability demands that an institution must be obligated to answer questions regarding its decisions or actions and there must also be means for enforcing consequences for failing to be accountable. The traditional oversight mechanisms over surveillance of communications and personal data by security agencies include official institutions such as courts of law, legislatures and statutory bodies. In many countries where surveillance has been gaining traction, the development of appropriate oversight mechanisms has been noted to be lagging, resulting in a vacuum of democratic oversight of security services (Duncan, 2022, p. 2). It is noted further, that in some states which have in place official oversight mechanisms, they often lack the power and resources to perform their oversight role effectively and efficiently. The lack of effective oversight mechanisms in the security sector puts at risk the respect for human rights and may also undermine the consolidation of democracy.

Duncan (2022, pp. 37–9) argues that security-intelligence authorities in the Southern African region are susceptible to state capture, and often protect the sitting Heads of State and not the citizenry. She observes that security services in the region often resort to harassment, persecution and violence against critics of the incumbent political party or faction of the ruling party. In Botswana, there have been concerns over the years that security services use surveillance in an arbitrary and unlawful manner (Mogapi, 2024). The prevailing situation is partly attributed to weak and/or ineffective traditional oversight mechanisms, which include courts of law, the legislature and statutory bodies. The weakness of the traditional oversight mechanisms makes it necessary to explore other oversight mechanisms to complement the traditional ones, such as popular agency (Interview with Mogwe, 2024). Popular agency oversight of the intelligence sector can contribute significantly to good governance and accountability in the sector. Popular agency acts as a watchdog against government through, inter alia, monitoring government performance, contributing to policy formulation and monitoring compliance with law and human-rights observance (Cole et al., 2008, p. 11).

This chapter explores popular-agency oversight of the security sector in Botswana. To appreciate the call for the strengthening of popular oversight, the chapter shall give an overview of intelligence oversight in the country, highlighting the oversight deficit. The chapter will also give a case study of what is arguably a success story of public oversight and will assess the strengths and weaknesses of popular agency in the country. In January 2023 the combined efforts of CSOs and the media forced the Minister of Defence, Justice and Security to amend some controversial clauses in the Criminal Procedure and Evidence (Controlled Investigations) Bill No. 1 of 2022. This chapter draws from published primary and secondary sources, as well as interviews with targeted interviewees. The writer targeted people who have knowledge of operations of intelligence services, media practitioners who have been targets of surveillance and those that have written stories on the subject, practising attorneys who have represented targets of surveillance and civil society activists.

Overview of the intelligence sector in Botswana: Development of the sector

There are several security-sector agencies in the country that are tasked with the role of ensuring the security and stability of the state by preventing internal and external threats. These agencies include the Directorate of Intelligence and Security (DIS), the Directorate of Corruption and Economic Crime (DCEC), the Special Branch of the Botswana Police Service (BPS) and the Military Intelligence of the Botswana Defence Force (BDF). Commentators on the security sector point to a lack of accountability of these agencies in the execution of their mandates, a factor attributed to how these agencies are governed and their perceived politicisation (Gwatiwa and Tsholofelo, 2021, pp. 190–1). This raises the question of the effectiveness of oversight mechanisms for these agencies. For one to appreciate the governance and culture of the security sector in Botswana, it is imperative to understand the evolution of the sector.

The country now known as Botswana was declared a British Protectorate, Bechuanaland Protectorate, in 1885. It was ruled directly by Britain through a High Commissioner until it was granted independence on 30 September 1966. Gwatiwa and Tsholofelo (2021, p. 192) posit that the culture of politicisation of security services dates to the colonial days. At that time, intelligence collection centred around Pan-Africanist activities at a time when colonies were agitating for independence. Colonial authorities considered efforts by Pan-African activists in their quest to gain independence a threat to the establishment, hence a threat to state security. National security interests were centred around the preservation of the colonial administration. Activities of nationalist movements to gain independence were thus viewed as national security threats as they threatened the continued existence of the colonial administration. In 1956 the United Kingdom Colonial Office under the Home Office (through the UK Security Office), issued a circular to all colonies and protectorates calling for the development of strong, organised intelligence structures (Kgosi, 2006, pp. 47–9). The circular required territories to furnish the UK Security Office in London with monthly intelligence reports containing regular and comprehensive collation of information, including, among others, activities of nationalist movements, local societies and organisations and, in particular, communist activities (Colonial Office, 1956). The circular further elaborated that typical points to be covered in the reports were to include:

- Communism – the Communist Party or local communist group, policy, influence, finances and external links, party’s penetration of labour, education, government departments, essential services and security forces.
- Extremist nationalism – policy and influence of parties, subversive agitation, external links and terrorism.
- Labour and agrarian unrest – general economic conditions, labour disputes and grievances and exploitation by political groups.
- Radical, religious and tribal tension – xenophobia and anti-colour bar agitation, religious cults and disputes, and intertribal disputes.
- Frontier and border incidents – trans-frontier raids, grazing disputes and frontier incidents.

The Bechuanaland Protectorate established a Special Branch in 1963 as a unit of the Protectorate police force. This was to be the intelligence department of the police and an instrument for the collection and assessment of any information that may affect the security of the territory. The main duties of the Special Branch included:

i) Collecting, processing and assessing information on subversive and potentially subversive organisations and connected personalities from all available sources.
ii) Planning, acting and advising on counter-subversive and counter-espionage operations.
iii) Advising government, where appropriate, through the Intelligence Committee on matters relating to protective security and the use of security intelligence.
iv) Assisting the Criminal Investigation Department of the police in the investigation of any criminal offence having a political or subversive complexion and to work closely with the district administration (Bechuanaland Protectorate Police Special Branch Directive No. 2, 1964).

It is apparent from the circumstances surrounding the formation of the Special Branch and its mandate that during the colonial period, the threat perception was mainly domestic and regional and/or international threats were important only if they threatened the strategic ambitions of the colonial establishment (Gwatiwa and Tsholofelo, 2021, p. 193). The head of the Special Branch was responsible to the Commissioner of Police. He/she was a member of the Central Intelligence Committee (CICC) and had access, as required, to heads of departments. The government secretary was, however, the main channel for the provision of intelligence reports to the government. The use of the Special Branch as an intelligence agency meant that as a branch of the police, it combined both mandates of intelligence gathering and executive powers of enforcement through arrests (Tsholofelo, 2014, p. 6). Assigning both powers to a single entity is not ideal, as it does not provide for checks and balances in the authority's use of the powers. There were no clear mechanisms put in place to provide oversight of the Special Branch.

When Botswana gained independence in 1966, the Special Branch was retained as the main intelligence agency, and in January 1968, the government issued a directive formulating a Charter of the Botswana Police Special Branch. Directives are not legislation or subordinate legislation; they belong to a body of rules which are of great practical importance to guide the conduct of officials in the exercise of their powers (Baxter, 1991, p. 200). The Charter laid down in general terms the duties of the Special Branch as follows:

a) Security intelligence – obtaining, collection, appreciation and dissemination of all intelligence relating to subversive movements, organisations and individuals that may assist the government in the maintenance of national security.
b) Protective security – protection of information, material, personnel and, where necessary, operations. This included such matters as the proper handling of classified information, counter-sabotage, the protection of vital points, security and similar matters and the tendering of advice to the government.
c) Counter-espionage – detection, penetration and control, in cooperation with the security service, of foreign intelligence organisations that may operate within or against the country.
d) In cooperation with government departments concerned, arrange for the collation, appreciation and dissemination of intelligence regarding the activities of political, commercial and other organisations, and associations or persons that may be of security interest.
e) Liaise with other government departments and stay connected with public opinion on matters that are likely to cause general discontent among the public and dissatisfaction with government measures or government policy (Kgosi, 2006, pp. 51–2).

The Head of the Special Branch, usually a Deputy Commissioner of Police, was responsible to the Commissioner of Police for the effective discharge of his/her duties. The Head of the Special Branch had a deputy and other officers and personnel working under him/her. At district level, the country was divided into regions headed by an Assistant Commissioner of Police, who reported to the head of the Special Branch. In 1998 the Special Branch changed its name to the Security Intelligence Services. It is, however, said that the change was mainly only in name and did not affect its mandate (Gwatiwa and Tsholofelo, 2021, p. 194). A conspicuous omission in the Charter on the Special Branch was that nothing is said on oversight of the agency.

Security threats to the state post-independence were perceived to comprise, inter alia:

- Communisms and communist-inspired activities.
- Pan-Africanist activities.
- Labour unions as well as opposition by local chiefs who resented the erosion of their traditional powers.

Mogalakwe (2013, pp. 12–27) argues that the security threats perception was not surprising as it reflected the realities of state-making and nation-building in the then nascent state. It is also observed that while post-independence domestic dissent was no longer considered a national security matter, it did not stop the security agencies from subjecting those who were not in agreement with the ruling party or faction of the ruling to surveillance. The late Dr Kenneth Koma, a leading opposition leader, was kept under surveillance throughout his political life (Magang, 2008, p. 471). It is further noted that the Special Branch used to keep a faction of the ruling Botswana Democratic Party which had fallen out of favour with the party leadership under surveillance. The faction was not engaging in anything subversive or unlawful or which could be said to be posing a threat to the security of the state, as they were canvassing for support for their preferred candidates, a normal democratic activity (Magang, 2008, p. 388 and p. 593). The practice was clearly a relic of a culture that had developed during the colonial administration where dissent with the powers that be was considered a threat to the security of the state.

The overview of the development of the security sector reveals that the issue of oversight was neglected both pre- and post-independence. Given the nature of security agencies and the work they do which often require them to resort to covert and intrusive means that may infringe upon civil liberties, oversight of the sector is critical for ensuring that these institutions both contribute to the protection of the populations they serve and respect the rule of law and human rights. Post-independence, one would have expected a change of attitude and culture in the governance of the security sector influenced by the democratic ethos that the State of Botswana had embraced at independence. The State of Botswana has been affirmed as a civilised state established under democratic principles whose bedrock is the rule of law (*Good v Attorney General (2),* 2005, p. 357). Unfortunately, until the establishment of the DIS, the issue of oversight of the security sector was not formally addressed even for the DCEC, which is established by statute.

Oversight is important as it provides an assurance of legality, proportionality and propriety for activities of the security sector. Lack of oversight of the security sector in Botswana has made it susceptible to state capture, where the agencies tend to protect the interests of the sitting Head of State, rather than the citizenry. The situation is not helped by the general attitude of the courts when national security is raised. The traditional approach of the courts has been that it is the responsibility of the executive to determine what constitutes a threat to national security and, when the executive has exercised its discretion, it is not the business of the courts to second-guess it (*Good v Attorney General (2),* 2005, pp. 357–62). Recent decisions of the Court of Appeal, however, give optimism that the apex court may be drifting away from the conservative approach. In a recent decision, the court has held that 'Whether or not an investigative functionary entertains a belief, on reasonable grounds, as to the commission of a crime is a justiciable matter to be objectively tested by the courts' (*Director General of the Directorate of Intelligence and Security and others v Seretse Khama Ian Khama*, 2022, para. 46). The essence of the judgement is that where an investigative authority wishes to obtain a warrant from the courts to investigate a matter relating to national security, it must furnish the court with proof of the existence of such belief. An investigative authority will be required to establish facts or state of affairs, which, objectively viewed, must exist before a court can grant a warrant (*Attorney General v Paul,* 2019, p. 435). If a court finds that, objectively, the facts relating to national security do not exist, it will not issue a warrant. While the developments are welcome, the major concern remains the lack of a clear definition of national security in the country. This leaves courts without clear national norms upon which they can objectively determine whether national security is at stake.

In the mid-90s, in response to new security challenges such as terrorism and readiness to deal with contemporary security threats in the country and globally, discussions within government commenced on the setting-up of an independent intelligence organisation (Kgosi, 2006, p. 53). The security environment had evolved globally, and the Security Intelligence Services was finding it difficult to forge partnerships with international counterparts as it was only a police service (Tsholofelo, 2014, p. 5). The discussions culminated in the birth of the DIS, which was supposed to be an independent institution. The functions of the DIS include:

a) Investigate, gather, co-ordinate, evaluate, correlate, interpret, disseminate, and store information, whether inside or outside Botswana, for the purposes of: –
   i) detecting and identifying any threat or potential threat to national security,
   ii) advising the president and the government of any threat or potential threat to national security,
   iii) taking steps to protect the security interests of Botswana, whether political, military or economic;

b) Gather ministerial intelligence at the request of any government ministry, department or agency and, without delay, evaluate and transmit as appropriate to that ministry, department or regulate, in cooperation with any government ministry, department or agency entrusted with any aspect of the maintenance of national security, the flow of intelligence and security, and the co-ordination between the Directorate and that ministry, department or agency of functions relating to such intelligence;

c) Advise government, public bodies, and statutory bodies on the protection of vital installations and classified documents;

d) Make recommendations to the president in connection with: –

   i) policies concerning intelligence and security,

   ii) intelligence and security priorities, and

   iii) security measures in government ministries, departments or agencies.

It is worth noting that, like the Special Branch, the DIS performs both intelligence and executive functions. The agency is tasked with the gathering, evaluation and dissemination of information and, at the same time, has the executive powers of arrest and searches.

The Intelligence Security Service Act, 2007 (ISS Act) adopts a broad definition of national security, which includes political, societal and economic threats. Tsholofelo (2014, p. 6) warns that we should be wary of the broad definition of 'national security', as it has tended to be abused in the past. He further cautions that defining threats to national security by reference to acts relating to subversion and terrorism may pose challenges as the parameters of these two terms are problematic. Gill (2005, pp. 12–33) also warns that the term subversion if not properly qualified can mean anything, including political and labour movements' activities that are both lawful and peaceful. Furthermore, the definition of terrorism remains contested globally, which could lead to the easy abuse of the concept. In Botswana, it has been recorded that in the past; the Special Branch engaged in the surveillance of a prominent opposition political figure and a faction of the ruling part that had fallen out of favour with the party leadership. In June 2024 a local newspaper reported that the DIS was monitoring some ruling party Members of Parliament who were planning to oppose a controversial government-sponsored constitutional amendment bill (Weekend Post, 1–7 June 2024). These activities were presumably monitored by the security services under the veneer of being subversive, but these are clearly lawful exercises of rights guaranteed under the Constitution.

Oversight deficit in the security sector

The ISS Act establishes some mechanisms that are supposedly intended to provide oversight, direction and guidance to the DIS. In a democratic dispensation, intelligence governance spreads responsibilities of control and oversight between the various arms of government (Bruneau and Boraz, 2007, p. 14). These include executive control, legislative oversight, judicial review and internal control (Tsholofelo, 2014, p. 8). The ISS Act attempts to embrace these measures.

Executive control of the DIS is provided by the CIC. This is a 13-member committee chaired by the President and includes, among others, the Vice President, ministers responsible for intelligence and security, and foreign affairs, respectively, and heads of both the BPS and the BDF. The function of the CIC is to guide the DIS on matters relating to national security and intelligence interests and advise the President on policy and policy formulation in the interests of national security. Members of the CIC are all presidential appointees, which has raised concerns over its independence. Another contentious issue is the unilateral appointment of the Director General (DG) of the DIS by the President, which has led to concerns that he/she may appoint someone at his/her own personal bidding instead of the national interest (Tsholofelo, 2014, p. 9). These concerns have arguably been confirmed when the Court of Appeal found that the DIS had unlawfully attempted to usurp the powers of the DCEC in investigating corruption (*Attorney General v Katlholo*, 2024, p. 21). In this case, the DIS had attempted to get access to confidential files of an investigation into alleged acts of corruption in respect of a company linked to former President Ian Khama's brothers. The fallout between President Masisi and Khama is well documented, and the former is on a self-imposed exile in South Africa. It must be noted that the former DIS DG, Colonel (rtd) Kgosi, who is believed to be close to Khama, was unceremoniously dismissed from office by President Masisi and replaced with the current DG, Brigadier (rtd) Magosi. The rift between the incumbent President and his predecessor and its effect on the DIS and society at large is aptly captured by Judge Kebonang of the High Court in one of the several cases that the DIS has been brought against the former DG. In describing the case, the Judge said:

> It is one of mutual dislike and mistrust between a spy agency and its former spymaster. This has negatively affected the smooth functioning of the different agencies in the web of government. Every facet of public and private life has felt this impasse. The fallout permeates every layer of government, and many careers and lives have been unfairly destroyed as a result. With no end in sight, it weighs on the rule of law and the sanctity of institutions (*Attorney General and others v Kgosi,* 2024, p. 2).

These cases give credence to concerns that President Masisi is using the DIS to settle personal scores. The Court of Appeal has found that the DIS under Magosi has acted as a law unto itself in breach of the very foundational tenets on which the state was established, and the respect for the rule of law when it usurped the powers of the DCEC by taking over the investigation of corruption (*Attorney General v Katlholo*, 2004). The cases also cast serious doubt on the ability of the executive to guide and control the DIS to act in accordance with the law. Equally concerning is the silence of the executive on the governance of the DIS in the aftermath of the damning remarks by judges about the institution. It is reported that some Botswana Democratic Party elders tried to raise the matter of the DIS DG's perpetual negative public image with President Masisi, but he declined to discuss the matter with them (Weekend Post, 6–12, July 2024, p. 3).

Legislative oversight of the DIS comes in the form of the Parliamentary Committee on Intelligence and Security (PCIS). The committee consists of nine Members of Parliament who are not Cabinet members appointed by the President after consulting the Leader of the Opposition. The mandate of the PCIS is limited in that it is only tasked with examining the expenditure, administration and policy of the DIS. The committee does not have an oversight of the activities or operations of the institution. The independence of the PCIS is also questionable. Unlike other parliamentary committees whose members are appointed by the Parliamentary Selection Committee, members of the PCIS are appointed by the President and it reports to him/her annually on the discharge of its functions. The PCIS's limited mandate and lack of independence has led to opposition Members of Parliament refusing to be appointed to the committee. After the 2019 general elections, the President attempted to constitute the PCIS and invited members of the opposition, but they declined with the then Leader of the Opposition, Dumelang Saleshando, saying the ISS Act was never intended to deliver an institution that is subjected to parliamentary scrutiny and oversight and, therefore, found it fruitless to be appointed to the PCIS as it does not play any meaningful oversight of the DIS (*The Botswana Gazette*, 12 November 2020).

The ISS Act provides for judicial oversight of the DIS in the form of a Tribunal. The Tribunal is established to receive and adjudicate complaints from any person who feels aggrieved by an act or omission of an officer of the DIS. Members of the Tribunal are appointed by the President after consultation with the Leader of the Opposition, and consist of three members: a judge or retired judge of the High Court, or a legal practitioner who qualifies to be appointed as a judge of the High Court, and two other persons, one of whom shall have considerable knowledge of the subject matter of the complaint and operation of security agencies. The independence of the Tribunal has been queried, with the major concern being the President's involvement in the appointment of its members (Tsholofelo, 2014, p. 11). The Tribunal suffers a credibility crisis, a factor that may have contributed to it receiving very few cases since its establishment. The Tribunal is not permitted to inquire into any complaint it considers prejudicial to national security. What constitutes national security has remained ambiguous and contentious in the country as there is no national security strategy or policy in place which can guide the Tribunal in determining whether a complaint would be prejudicial to national security.

Judicial oversight of the DIS further comes in the form of a requirement of a warrant in cases where there is need by the institution to use intrusive methods in the investigation of threats to national security. In such cases, the institution must apply to a Senior Magistrate or High Court for a warrant. There, however, continues to be persistent public concerns that, even though the Act requires the DIS to obtain a warrant to intercept communications, the institution is still monitoring activities of opposition politicians, journalists and civil society activists without authorisation. There is no information publicly available on the use of this provision and there is need for transparency in its use to promote accountability of the DIS.

Internal controls are rules and processes within an institution aimed at ensuring that staff perform their mandate professionally and effectively within the limits of their authority and in compliance with the law (DCAF-Geneva Centre for Security Sector Governance, 2022, p. 6). Internal controls usually take the form of i) inspectors general, ii) professional ethos and institutional norms and iii) multiple intelligence organisations (Bruneau and Boraz, 2007, pp. 15–16). The DIS does not have an inspector general. The Intelligence and Security Council (ISC) established in the ISS Act appears to be somewhat playing the role. The functions of this committee include reviewing activities of the DIS and receiving and examining complaints lodged by members of the agency. Membership of the ISC consists of the Permanent Secretary to the President, the Attorney General, the DIS DG and the Deputy DG. It is reported that in the past, the ISC has reviewed punishments meted out to officers in terms of the disciplinary code of conduct (Tsholofelo, 2014, p. 12). The presence of both the DG and the deputy in the ISC is anomalous as the two may be conflicted when the committee is reviewing the activities of the institution or sanctions meted out to officers in breach of the code. It is reported that the DIS has in place a code of conduct for its officers; however, the code has not been made public (Tsholofelo, 2014, p. 12).

The security sector in Botswana has always been marred by controversy relating to its poor governance, resulting in them not being accountable for the performance of their mandate. While the DIS was supposed to be an independent institution when its formation was under discussion, since its inception it has been embroiled in controversy. The controversy emanates from its poor governance and politicisation and, thus, lack of accountability in the performance of its duties. This trait is a colonial relic and a legacy of the Special Branch. During the protectorate era, the colonial administration used national security surveillance as a tool for social and political control. The focus was on Pan-Africanist activities which were threatening the colonial interests, and communism. Post-independence, one would have expected a change of attitude in the determination of threats to the security of the state. Unfortunately, it appears that intelligence agencies have not changed their attitudes resulting in them carrying out their functions in a manner that is not consistent with democratic ethos, thereby undermining civil liberties. The prevailing situation is exacerbated by poor and/or inadequate oversight mechanisms on the sector. In the case of *Attorney General v Katlholo*, referring to attempts by the DIS to encroach on the mandate of the DCEC, the court observed: 'This case concerns an egregious excess of authority and cry out for rectification and rebuke.' It is the responsibility of oversight mechanisms to perform the task of rectification and rebuking any rogue intelligence sector agency. The courts are playing their part, but it seems the other oversight mechanisms on the DIS established under the Act are failing. The status quo makes a compelling case for the strengthening of public oversight of the sector.

A case study of public oversight

Public oversight of the intelligence sector is performed by CSOs and the media. These institutions contribute to promoting good governance and accountability by acting as watchdogs against government, contributing to policy formulation and monitoring compliance with human-rights norms and standards (Cole et al, 2008, p. 1). The media is expected to disseminate and scrutinise information about governmental activities, including those of the intelligence sector, bringing issues into the public domain for debate. The media can draw public and political attention to human-rights infringements, abuse of power and lack of accountability (Hillebrand, 2012, p. 693). When the media exposes cases of malpractices and/or alleged malpractices in the intelligence sector, this may contribute to public debate. The media may also be a channel for whistleblowers to expose wrongdoing in the intelligence sector, especially where there are non-existent or weak oversight mechanisms on the sector. CSOs on the other hand play an important oversight role on the intelligence sector in several ways. These organisations may make submissions when the legislature is adopting or amending laws governing the sector by drawing attention to flaws and campaign for inclusion of provisions that are consistent with international human-rights norms and standards in the proposed law. In some countries CSOs have taken part in initiating or intervening in litigation relating to the intelligence sector before national courts and international tribunals (Council of Europe, 2015, p. 59). Like the media, CSOs equally play a watchdog role by monitoring government actions and work of oversight mechanisms in the intelligence sector.

CSOs and the media in Botswana have and continue to play a meaningful public oversight role on the intelligence sector. Their success may be debatable, but one incident of significance where the combined efforts of CSOs and the media culminated in partial success is worth narrating. On 12 January 2022, the Minister of Defence, Justice and Security published in the *Government Gazette Extraordinary* (Vol. LX. No. 3) the Criminal Procedure and Evidence (Controlled Investigations) Bill, 2022, Bill No. 1 of 2021. The Bill was expedited through the National Assembly under a certificate of urgency. The justification for the expedited procedure was said to be the need for the country to meet requirements of the Financial Action Task Force (FTAF), which had blacklisted the State of Botswana, which had been found to be non-compliant with FATF standards. The Bill had six parts, with the pertinent ones being:

- Part II provided for an undercover operations framework and formalised the collection of information through undercover operations orders and assumed identities.
- Part III dealt with interception of communications framework, authorising the interception of communications by investigatory authorities, and set out the role of service providers in controlled investigations for the gathering of criminal evidence.
- Part IV introduced provisions for the handling of information in controlled investigations.

Introducing the Bill for the Second Reading in the National Assembly, the Minister said, among other things, that the Bill was in response to a recommendation of the FATF, which had identified that there was no explicit provision for the use of undercover operations in the country (Hansard, 2022, p. 63). Following the publication of the Bill and before its Second Reading in the National Assembly, the Bill was met with shock and resistance from the media, CSOs and the public (Southern Africa Digital Rights, 2022). The Bill had several troubling clauses and omissions. It gave a head of an investigatory authority who believed, on reasonable grounds, that a delay in obtaining an undercover warrant would defeat the object of the undercover operation, to authorise an investigating officer to engage in undercover operation. Similar powers were also given to a head of an investigatory authority for the interception of communications. The Bill did not provide for adequate oversight mechanisms on the use of these intrusive investigation methods. For example, it did not provide for judicial oversight.

The Bill received widespread criticism from local media and CSOs such as the Media Institute of Southern Africa (Botswana Chapter), Botswana Editors Forum, and Ditshwanelo – the Botswana Centre for Human Rights. The concerns raised against the Bill were that its enactment would negatively impact the protection of fundamental rights such as privacy, freedom of expression and freedom of association. Furthermore, the Bill did not provide adequate oversight mechanisms to guard against abuse of powers given to investigatory authorities. It was argued that giving powers to heads of investigatory authorities to authorise the use of intrusive investigatory methods without court supervision was prone to abuse. The government was also criticised for opting to have the Bill taken through the National Assembly under a certificate of urgency, thereby depriving the public of sufficient time to interrogate and scrutinise the Bill. The strategy adopted by those opposing the Bill was, first they met Members of Parliament both from the ruling party and opposition to brief them on the dangers of the proposed law. They emphasised to the Members of Parliament that their opposition to the Bill was not a partisan matter but was motivated by the dangers the proposed law posed if it were to become law. After meeting the Members of Parliament, the activists published alerts locally, regionally and internationally, in which they highlighted the dangers the proposed law posed to the enjoyment of the fundamental rights and freedom of the individual. The campaign against the Bill received regional and international support. The Botswana Editors Forum coordinated activism against the Bill, and for about 1.5 weeks, it hosted experts from Lesotho, Namibia, Swaziland, South Africa and Zimbabwe to assist in strategising against the Bill. Statements against the proposed law were published in local media and protest letters were written to the President, the Speaker of the National Assembly and the Minister of Defence, Justice and Security. In its solidarity message, the African Editors Forum wrote, 'The Bill will allow the government to spy on citizens without a warrant and supervision from the courts. This is a direct move to subvert democracy and violate the rights of the media to do its work freely and the rights of Botswana to freely receive information' (Committee to Protect Journalists, 2020).

The combined efforts of opposition and protest against the Bill ultimately forced the Minister of Defence, Justice and Security to effect amendments that partly addressed the concerns over the Bill. The Minister's deference to public pressure was commendable and a significant victory for public oversight in a matter relating to governance of the intelligence sector. When presenting the Bill for the Second Reading in the National Assembly, the Minister conceded:

> I am aware that the Bill has caused uneasiness and bearing this in mind together with concerns raised by this Honourable House, I have re-examined the Bill. I will, therefore, be presenting some amendments during the Committee Stage. I wish to assure this Honourable House and Batswana that I have heard you and I would like to make it categorically clear that there is no intention to diminish the rule of law (Hansard, 2022, p. 63).

The Minister emphasised to the House that he was aware that intrusive investigation techniques must be used as a last resort. He assured the National Assembly that the amendments he was going to make to the Bill would be aimed at setting stringent standards by outlining matters that must be considered by a court before which there is an application for a warrant to conduct intrusive investigation methods. True to his word, the Minister did introduce some amendments to the Bill during the Committee Stage, some of which addressed the concerns raised against the original Bill. Notable amendments were:

a) The Bill was amended by deleting a clause that permitted a head of an investigatory authority to authorise an undercover operation without a warrant. The amendment went further to prohibit the use of undercover operation without a warrant and making it a criminal offence to conduct an undercover operation without a warrant. In recognising the intrusive nature of using undercover operation, and the need that it must only be done as a last resort, the Bill was amended by inserting a clause that requires that in an application for undercover operation, it must be demonstrated to the court that what is sought to be achieved by the warrant could not reasonably be achieved by other less intrusive means.

b) Amendments to the Bill were also effected to address concerns raised on powers given to heads of investigatory authorities in conducting interception of communications without a warrant. A new clause was inserted prohibiting the interception of communications without a warrant. Interception of communications without a warrant was made a criminal offence. Further amendments to the provisions relating to interception of communications were made to ensure that prior to the issuance of a warrant, a court must be satisfied that there is an actual threat to national security, or a serious crime-related activity is being or will be committed, or that there is potential threat to public safety. In making these amendments, the Minister highlighted that the issuance of a warrant of interception of communications is a method of investigation to be used under the most exceptional circumstances and as a last resort (Hansard, 2022, p. 65).

c) To strengthen oversight mechanisms, the Bill was also amended to include the establishment of a Controlled Investigations Coordinating Committee (CICC), chaired by a judge or retired judge and comprising people with knowledge and relevant experience. The functions of the CICC include protection of interception subjects and targets and to receive and determine complaints in respect of the use of warrants issued under the proposed law.

The Criminal Procedure and Evidence (Controlled Investigations) Bill was passed by the National Assembly on 4 February 2022. The amendments which the Minister had promised were incorporated into the Bill at the Committee Stage in the National Assembly. While the final law may not be perfect, an important lesson is the impact public oversight had in shaping the law that was finally passed by Parliament. The amendments made to the Bill owing to public intervention brought about important oversight measures on the intelligence sector. There is, however, still more work to be done by both the media and CSOs to ensure accountability in the intelligence sector. There is still a cloud of secrecy on the extent to which intrusive investigatory methods are used by the agencies. Although the Criminal Procedure and Evidence (Controlled Investigations) Act, 2022, prohibits the use of intrusive investigation methods without a warrant, there continues to be concerns that intelligence agencies are still using these methods unlawfully. Unfortunately, it is not possible to verify the concerns as the law does not provide for post-surveillance notification. Post-surveillance notification is an important oversight mechanism as it will show the prevalence of the use of intrusive methods and the subjects or targets of such measures. Armed with this information, one will be able to determine whether these measures are used reasonably or arbitrarily. For example, if information shows that most targets are media practitioners, this may raise concerns. There must be some level of transparency in the way intelligence agencies operate to allow the media and CSOs to perform their public-oversight functions. More worrying are findings that some intelligence agencies disregard the law which undermines the rule of law and democratic tenets.

For the media and CSOs to effectively perform their public-oversight role on the intelligence sector, there must be in place an environment in which they can challenge governments on sensitive matters without fear of harassment or retaliation (Council of Europe, 2015, p. 60). Public-oversight agencies in Botswana face several challenges which render their operating environment not ideal for the performance of their oversight role on the intelligence sector. There is apprehension among media practitioners and civil society activists that their digital communications and personal data are routinely monitored by the DIS. Two journalists interviewed by the writer said they were warned by whistleblowers within the DIS that the agency was monitoring their communications. They were not told whether such surveillance had been duly authorised, nor the purpose of such surveillance. The fear of being under surveillance by the DIS is also echoed by some civil society activists. The dark cloud of surveillance by intelligence agencies, whether real or perceived, has a chilling effect on the enjoyment of rights such as freedom of expression and association which are necessary to enable the media and CSOs to play their oversight role on the sector.

Surveillance of communications and personal data of members of popular agencies further poses threats to media freedom because it threatens the protection of confidential journalistic sources. In the execution of their public-oversight mandate, the media usually employs investigative journalism which often relies on confidential sources. Unlawful surveillance of journalists may undermine protection of sources as intelligence agents may be able to establish whom journalists have been communicating with, thereby leading to source identification.

There is a culture of secrecy surrounding the intelligence sector in Botswana which makes it difficult for CSOs and the media to access information on the sector, including policies. While some information on the intelligence sector must necessarily remain secret to ensure the efficiency of the services and protection of informants, it does not follow that all information about the sector must be withheld from the public. Information on the sector such as policies should be accessible to the public. The Constitution of Botswana does not guarantee a right of access to information and there is no law on the right. Public bodies, including intelligence agencies, are thus not obliged by law to disclose information on their policies or activities. The culture of secrecy in the intelligence sector is reinforced by a lack of a clear definition of the concept of national security. The Court of Appeal has held that it is for the executive to decide what national security is. It appears that security agencies are taking full advantage of this and treat almost any information on the sector as a national security matter. The DIS is leveraging on the loophole and has been using the national security mantra in matters that have no bearing on the security of the state as demonstrated in the *Attorney General v Katlholo* case. It would not be far-fetched to assume that surveillance of journalists, civil society activists and opposition politicians was/is done under the guise of protecting national security when, in essence, it was or is just for the protection of the interests of the sitting President.

In the fight against the Criminal Procedure and Evidence (Controlled Investigations) Bill, local CSOs and the media brought in regional and international partners. Part of the reason for bringing in outside partners was because it was felt by the coordinators of the resistance campaign that Botswana does not have non-governmental organizations (NGOs) with requisite skills, competencies and expertise to play an effective oversight role on the intelligence sector (Mogapi, 2024). Currently, Distshwanelo – The Botswana Centre for Human Rights – is the only one that engages in general human-rights advocacy. The organisation, however, has not been active in intelligence-sector oversight, except in isolated cases, where it has issued statements when a major event in the sector had occurred, like when the Criminal Procedure and Evidence (Controlled Investigations) Bill was published. The Botswana Centre for Public Integrity, while its mandate is the promotion of accountability in governance, is yet to expand its scope of activities to cover the intelligence-sector oversight (Interview with Seabo and Gaolebale, 2024). The NGO sector is mainly dependent on donor funding. The programmes that NGOs engage in are shaped and driven by interests and priorities of the donors. The Executive Director Ditshwanelo explains this point further: 'Because the funding comes from outside, it means we are often faced with having to make decisions about the relevance of the topic which is being funded or issues which are being funded or being prioritised by the funder' (Interview with Mogwe, 2024). Donor funding in the country is dwindling as Botswana is classified as an upper-middle-income country, leaving many NGOs dependent on government funding through the Botswana Council of Non-governmental Organisations (BOCONGO). Dependence of NGOs on state funding may compromise their independence, as it may make them shy away from criticising the state and its organs out of fear of losing funding. The possibility of state capture of NGOs that comes with funding of these institutions by government has led one civil society activist to vehemently oppose government funding (Interview with Mogwe, 2024).

The media in the country face hurdles on their ability to play an oversight role on the intelligence sector. The oversight comes, among others, in the form of investigative stories that expose malpractices in the sector. Quality investigative journalism requires resources and experienced journalists. Unfortunately, many of them are deserting the profession for better opportunities, leaving the industry with inexperienced journalists (African Media Barometer, 2023, p. 52). Media houses also face sustainability challenges arising from dwindling advertising revenue. The decline in advertising revenue means that traditional media have limited resources to invest in the production of quality news. They have resource constraints making it difficult for them to retain experienced journalists. Technological evolution has radically changed how news and other media content are produced and disseminated. The evolution has, in turn, affected the economic reality of journalism (Council of Europe, 2022). Advertising spending, which is an important source of revenue for the media, has shifted from traditional media to online platforms. The media in Botswana has not been spared this development. The media scramble for the few advertisers left, with the public sector being the largest. A media that is dependent on public advertising tends to avoid reporting on sensitive subjects like the surveillance sector because they do not want to earn the wrath of the government, resulting in a possible loss of advertising (African Media Barometer, 2023, p. 35). The predicament of a media that is overly dependent on advertising revenue is eloquently captured by the chairperson of the Botswana Editors Forum in the following words: 'Journalists are scared of repercussions, not only repercussions of surveillance, but repercussions of being isolated and targeted in terms of financial sanctions' (Interview with Mutapati, 2024).

A combination of the above two factors is depriving the media the use of an important oversight tool in the form of quality investigative journalism. The lack of experienced investigative journalists, and limited resources (if any) allocated to investigative journalism has an adverse effect on the quality of content we receive from the media.

The absence of clear legal protection for journalistic confidential sources of information discourages the media from investigating and writing stories on the intelligence sector because their sources can be easily identified. Protection of journalistic sources of information is now considered to be an aspect of media freedom (ACHPR, 2019, principle 25). Media freedom is guaranteed in the Constitution of Botswana, but there is no law that deals specifically with protection of sources. In view of the prevalence of the use of surveillance by intelligence agencies on the media and the absence of a law addressing protection of sources, this has a negative effect on the media's ability to play an oversight role on the intelligence sector. There is also a worrying trend in the country where intelligence agents raid newsrooms and confiscate journalists' communications and information-storage devices like computers, laptops and mobile phones. For example, in July 2023 agents from the DIS raided the offices of *Mmegi* newspaper, confiscating laptops and phones of the editor and a reporter, and took them for questioning (Committee to Protect Journalists, 2023). The two were later released without any charges laid against them and their gadgets were returned, but the journalists refused to take back the gadgets, resulting in the DIS giving then money to buy replacements. To compound matters, several newsrooms report that intelligence agents have infiltrated them. The absence of a law protecting sources and raids on newsrooms make investigative journalists an elevated risk to use as an oversight tool. The chairperson of the Botswana Editors Forum makes the following observation regarding the prevailing operating environment of the media in the country:

> Journalists tend to shy away when it comes to serious investigations. They tend to be scared to tackle those. You end up just writing simple things that are not going to put you in trouble because you know that at any time your gadgets can be grabbed. And, also, journalists know that they can be watched, they can be tracked, so, they know that intelligence officers at any given time, can know where they are, who they are meeting (Interview with Mutapati, 2024).

The ability of popular agencies, CSOs and the media to play an effective oversight of the intelligence sector further depends on their independence and integrity. The discussion above points to the compromised independence of both the media and NGOs in the country. The lack of independence stems mainly from financial vulnerabilities of both sectors and their dependence on the state. The media also suffers from credibility issues. The print media, in particular, has been said to be unprofessional and biased. Joel Konopo, a former editor, and co-founder of the INK Centre for Investigative Journalism, makes the following observation:

> There are constant complaints about bias, from readers and politicians alike. These complaints are not groundless. As director of Botswana's only independent investigative journalism unit, and a former newspaper editor, I have seen first-hand how the narrative offered by journalists in Botswana is all too often directly influenced by politicians; and how the close relationship between politicians and journalists leave the media too weak to hold the powerful to account (*Mail and Guardian*, 29 January 2020).

It will be anomalous to expect the media to play an oversight role on the intelligence sector when the media itself is not accountable and credible. If the media is not accountable, it has no moral ground to act as a watchdog over the intelligence sector.

Conclusion

The oversight deficit in the intelligence sector clearly makes a case for the strengthening of popular agency on the sector in Botswana. The recent Court of Appeal ruling that the DIS has been abusing its powers and encroaching on the mandates of other security-sector agencies under the guise of protecting national security, and the fact that all this took place under the nose of the formal DIS oversight mechanisms, makes the case for popular agency more urgent. The success of popular agency in the campaign against the Criminal Procedure and Evidence (Controlled Investigations) Bill is testimony to the power that these agencies have in promoting accountability in the intelligence sector. Had it not been for popular agency intervention, the legislature could have enacted a law giving unlimited powers to heads of investigatory agencies to authorise use of intrusive methods of investigation without adequate safeguards. But for popular agencies to perform their role effectively, the operating environment must be conducive. This chapter has identified some of the challenges facing popular agencies, which need to be addressed to create the right environment for these agencies to perform their mandate:

- They need to be assured financial sustainability to ensure that they are not overly dependent on the state for survival. Financial stability will enhance the popular agencies' independence from the state. There are several options that can be used. NGOs can be funded directly by the legislature in a way that will insulate them from political meddling. Measures can also be put in place to promote media sustainability, like according preferential tax rates to media companies and putting in place support measures for investigative journalism.
- The right to information must be protected in law and practice. A law protecting this right must create a duty to proactively disclose information in the custody of public bodies and relevant private bodies. The law must apply to the intelligence sector and exemptions to disclosure should only be legitimate where the harm to the interest protected demonstrably outweighs the public interest. A right to information law would reverse the culture of secrecy in the intelligence sector.
- The legislature should enact a law that defines national security. The lack of a definition of this concept has allowed intelligence-sector agents to abuse the concept at the expense of protection of human rights. The definition of the national security should be anchored on international norms and standards to ensure that an appropriate balance is achieved between protection of genuine-national security interests and human rights.
- The legislature must pass a law protecting journalistic sources of information. A related issue is for a court to satisfy itself

before granting an order for a warrant of interception of communications of a journalist, that the interception will not unjustifiably lead to source identification.

- The media, especially the print media, need to rebuild its credibility so that they regain public trust. This will be achieved if the media puts in place credible and effective self-regulatory mechanisms that will enforce high ethical standards in the sector.

References

Attorney General v Good (2) [2005] 2 BLR 337 (CA).

Attorney General v Katlholo, CACGB-198-22, unreported decision of the Botswana Court of Appeal delivered on 28 June 2024.

Attorney General v Paul [2019] 2 BLR 421 (CA).

Baxter, L. 1991. *Administrative Law.* Cape Town: Juta & Co Ltd.

Borowiak, C.T. 2011. *Accountability and Democracy: The Pitfalls and Promise of Popular Control*. Oxford: Oxford University Press.

The Botswana Gazette. 2020. 'I will not be part of this fruitless DIS exercise' (12 November) available at: the gazette.news/opinion/i-will-not-be-part-of-this-fruitless-dis-exercise/

Botswana Parliament. 2021. *Daily Hansard: The First Meeting of the Third Session of the Twelfth Parliament.* 10 November 2021.

Botswana Parliament. 2022. *Daily Hansard*. 3 February 2022, pp. 63–5.

Botswana Special Branch Charter, POL. F. 2, Directive No. 2, dated 1 January 1968. Botswana Government Archives, Gaborone.

Bruneau, T.C. and Boraz, S.C.. Reforming Intelligence: Obstacles to Democratic Control and Effectiveness. Texas, University of Texas Press.

Burke_White, W.W. 2004. Human Rights and National Security: The Strategic Correlation, 17. Harvard Human Rights Journal, pp. 249 - 280.

Cole, E., Eppert, K. and Kinzelbach, K. 2008. *Public oversight of the security sector: A handbook for civil society organizations*. UNDP Bratislava Regional Centre; Geneva Centre for the Democratic Control of Armed Forces (DCAF). [Online]. [Accessed 10 August 2023]. Available from: https://www.undp.org/publications/public-oversight-security-sector-handbook-civil-society-organizations.

Colonial Office dispatch, Ref. ISD.65/1, Circular No. 458/56, dated 28 April 1956. Botswana Government Archives, Gaborone.

Committee to Protect Journalists. 2023. Botswana intelligence agents detain 2 journalists overnight. *Committee to Protect Journalists.* [Online]. [Accessed 13 August 2024]. Available from: https://cpj.org/2023/07/botswana-intelligence-agents-detain-2-journalists-overnight/.

Council of Europe. 2025. Democratic and effective oversight of national security services.. Strasbourg, Council of Europe.

Director General – Directorate of Intelligence and Security and Another v Seretse Khama Ian Khama, Civil Appeal No. CACCGB-315–21, unreported judgment of the Court of Appeal of Botswana delivered on 18 November 2022.

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

Friedrich-Ebert-Stiftung 2023. African Media Barometer: Botswana 2023. Windhoek, FES.

Gill, P. 2005. Establishing intelligence service accountability. In: Johnson, L.K. and Leigh, I. eds *Who's Watching the Spies?*, pp. 12–33.

Gwatiwa, T. and Tsholofelo, L. 2021. Civilian Intelligence Services in Botswana: Colonial legacies and politicization of the Directorate of Intelligence and Security. In: Shaffer, R. ed. *African Intelligence Services: Early Postcolonial and Contemporary Challenges*. Maryland: Rowman & Littlefield, pp. 189–208.

Hillebrand, C. 2012. The role of news media in intelligence oversight. *Intelligence and National Security.* 27(6), pp. 689–706.

Hutton, L. 2009. Intelligence and accountability in Africa. *Institute for Security Studies Policy Brief.*

Kgosi, I.S. 2006. Structuring African Intelligence Services: Special Reference to South Africa, Uganda and Botswana. Unpublished MA dissertation, Brunel Business School.

Magang, D. 2008. *The Magic of Perseverance*. Cape Town: CASAS.

Mogalakwe, M. 2013. Deconstructing National Security: The Case of Botswana. *Sacha Journal of Politics and Strategic Studies*. pp. 12–27. Vol. 3 (1)

Parsons, C. and Molnar, A. 2018. Government Surveillance: The Failures of Contemporary Canadian Interception Reports. *Canadian Journal of Law and Technology.* pp. 144–54. Vol. 16 (1)

R v Secretary of State, Ex parte Cheblak [2001] 1 WLR 877.

Tsholofelo, L. 2014. A Critical Evaluation of the Intelligence Oversight Regime in Botswana. Unpublished MA dissertation, Brunel University. Weekend Post. 2024. 'DIS blocks BDP rebels' (published in 01 -07 June 2024 edition).

INTERVIEWS

1. Interview with Ryder Gabathuse, Editor, *Mmegi* newspaper, 4 March 2024.
2. Interview with Unoda Mack, practising attorney, 4 March 2024.
3. Interview with Isack S. Kgosi, founding Director General of the Directorate of Intelligence and Security, 6 March 2024.
4. Interview with Tymon Katholo, former Director General of the Directorate on Corruption and Economic Crime, 19 March 2024.
5. Interview with Emang Mutapati, Chairperson of Botswana Editors Forum and Editor of *The Voice* newspaper, 19 March 2024.
6. Interview with Tumisang Seabo and Sonia Gaobolae, Botswana Integrity Centre, 20 March 2024.
7. Interview with Setho Mongatane, radio journalist, Gabz FM, 26 March 2024.
8. Interview with Spencer Mogapi, veteran journalist and former Deputy Editor of *Sunday Standard* newspaper, 26 March 2024.
9. Interview with Hon. Dithapelo Keorapetse, Member of Parliament and Leader of Opposition in Parliament, 6 June 2024.
10. Interview with Alice Mogwe, Executive Director, Ditshwanelo – The Botswana Centre for Human Rights, 11 June 2024.

CHAPTER FOUR

Public control and digital surveillance: Understanding the role of civil society in the DRC

Trésor Maheshe Musole

Introduction

In the Democratic Republic of Congo (DRC), civil society is one of the major players in the civic and democratic arena. It comprises all the organised forces in society outside the state, the family, political parties and the market. These are forces and structures such as associations, non-governmental organizations (NGOs), the press, trade unions, churches and universities (Abega, 2009). Over time, the goals of civil society have changed, owing to shifts in the country's social and political landscape, following similar patterns across three periods (Bugeme, 2020).

After the weakening of the welfare state in the 1970s and 1980s, as well as the agrarian crisis in 1980, civil society turned its attention to rural issues and community health, to the point of being described as 'local development brokers' (De Sardan, 1997). Around 1990, civil society became involved in human-rights issues as a result of development-aid conditionalities imposed on Southern African countries by donors. During the decade of war (1996–2006), the actions of civil society were characterised by a polarisation of discourse to the point of leading to an identity crisis, due to the personal positioning of certain players. From the second half of the 2000s, CSOs turned their attention to natural resources and the opening up of civic and democratic spaces. Faced with serious human-rights violations and strong competition for natural resources, civil society structures exerted strong pressure on the political and economic players concerned (Cappelle and Custers, 2009), to the point of changing public policies.

With the advent of new information and communication technologies, civil society players are facing new challenges in terms of civic and democratic space. This space has expanded to include online or web-based activities. Citizens are increasingly expressing themselves and exercising their political freedoms online wherever they happen to be. This exposes the structural limits of our democracies. Intelligence services are using electronic surveillance on an unprecedented scale to restrict civic space. Civil society actors, citizens' movements and political opposition are subject to a system of spying and electronic surveillance organised by state services (Maheshe and Mushagalusa, 2021), which is constantly increasing in societies (Salvas, 2001; Abu-Laban, 2014; Castagnino, 2018; Cornut St-Pierre, 2019; Camilla, 2020; Sfetcu, 2020; Vuilleumier, n.d.; Viana, 2021;).

However, civil society organisations in the DRC exert little or no pressure on these new forms of restrictions on civic space and digital democracy. As was the case in the area of sexual violence or the natural-resources sector, there is almost no public control on the part of civil society challenging unjustified secrecy by publicising abuses and organising awareness-raising campaigns. Official institutions such as the courts and parliament do not control this massive surveillance because they are highly politicised. The population is facing unprecedented restrictions on online civic space by government authorities. They justify these restrictions on the grounds of security on digital networks and claims of digital sovereignty. State services restrict civic space by resorting either to electronic surveillance of citizens or to control of the internet.

Faced with this situation, this chapter answers two questions:

1. What are the factors behind the low level of interest among Congolese civil society in the issue of surveillance?
2. How could civil society actions limit the abuses of surveillance?

To address these questions, the study first presents the organisation of Congolese civil society (IV) with the aim of identifying the factors that explain this low level of mobilisation in the face of electronic surveillance. Next, to explain the low level of interest in electronic surveillance among civil society organisations, the study draws on three case studies (V). Finally, the paper identifies the factors that explain civil society's lack of interest (V). Before addressing these questions, it is necessary to examine the methodology (II) and theoretical basis (III) on which this study is based.

Methodology

Understanding the role of civil society requires an appropriate, rigorous and operational methodological approach. The overall methodological approach is based on the systemic approach (Donnadieu and Karsky, 2002; Cambien, 2008). It is fundamentally qualitative, based essentially on documentary analysis, case studies and empirical data.

The literature review highlights the role of CSOs in electronic surveillance. Their organisation and functioning are studied with the aim of elucidating the role of these organisations and the factors explaining their inertia.

The qualitative survey contributes to the collection of empirical data by means of individual interviews. The interview narratives provide further depth to our analysis by means of a questionnaire survey. This methodological choice is explained by the desire to go beyond the framework of theoretical research and involve those on the ground facing the challenges of electronic surveillance.

The case study evaluates the actions of civil society with the aim of engaging CSOs in actions that limit the abuse of surveillance by establishing public control. The case study is understood as 'empirical research that studies a contemporary phenomenon in a real context, where the boundaries between the phenomena and the context are not clear' (Albarello, 2001). It is 'a particularly fruitful form of combination that brings together, in the field, data that can be distinguished around a social sequence circumscribed in space and time' (De Sardan, 2008). In this paper, the case studies will help to explain the role of civil society in the face of electronic surveillance.

Geographically, the scope of the presentation covers the DRC, focusing on the province of South Kivu. The province was chosen because of the dynamism and fighting spirit of its CSOs. According to Amuli, 'Local civil society in Kivu has been recognised for its combativeness since well before the period of the Sovereign National Conference, and it is above all the ONDGs that are the bearers of this dynamism' (Amuli et al., 2003).

In this province, six individual interviews were conducted with CSOs, lawyers, parliamentarians and so on. The information gathered was supplemented by two studies that had previously involved CSOs. One study looked at the role of civil society in mining governance. Forty-two individual interviews and 17 discussion groups were organised with FDHM's CSO partners, political and administrative authorities and stakeholders involved in the exploitation of mining resources (mining companies and mining cooperatives). In addition, 237 people were interviewed – 194 men and 43 women (CERDHO, 2022). The other studies the actions of CSOs working on natural resources in the DRC in the era of electronic surveillance: 10 individual interviews and 10 focus-group discussions (FG) were conducted with CSOs and citizens' movements working on mining governance in the DRC, security companies and mining companies operating in the sector and based in South Kivu.

Agency and the decolonial approach: The theoretical basis for understanding the role of CSOs

To understand the role of CSOs, the paper uses agency theory. The agency refers to a subject's ability to act autonomously and reflectively (Rebughini and Colombo, 2023). This refers to the possibility of acting in a dissident and innovative way against the forms of domination and construction observed in a society (Rebughini and Colombo, 2023). Theoretically, the doctrine distinguishes between two ways of understanding the notion of the agency. This paper draws on both approaches.

The first approach comes from Western thought, based on the theory of action. According to this theory, the causes of action lie in the actor's intention (Davidson, 1980). Intention implies a motivational commitment to action (Lyotard, 1991). This motivation is determined by the interests of the actors. Actors act according to whether or not their interests are affected. To understand the role of CSOs, this paper uses the theory of affected interests, which makes this motivational commitment more explicit. From a historical perspective, Annah Arendt associates intention with freedom, starting with Greek philosophy (Arendt, 1978). In ancient Greek society, absolute intentionality was outlawed (Rebughini and Colombo, 2023). In his work, Platon explains it in these terms: '*l'excès de la liberté amène à la tyrannie, qui est la confiscation de la liberté au profit d'un seul tyran. La vraie liberté est maîtrise des passions et obéissance à la raison*' (Platon, 1834). Ultimately, the agency is the freedom of the social actor in relation to social laws or the idea of the sovereign subject and his fantasy of completeness and autonomy (Rebughini and Colombo, 2023). Faced with the norms governing electronic surveillance in the DRC, CSOs are breaking free in order to regain their freedom to act. Resilience enables them to survive in a repressive environment.

A second approach to the agency comes from the American sociological tradition influenced by pragmatism. According to this approach, the agency is not based on the subject, but rather on action. This conception rejects the agent/structure dualism (Rebughini and Colombo, 2023). It involves a decentring or deconstruction of the subject. The agency implies a relational process of contextualised interaction and not a permanent struggle between the agent and social structures (Goodman, 1995). As such, action is influenced by the cultural and material characteristics of the environment (Rebughini and Colombo, 2023). In this way, the agency ceases to be an ideal characterised by the agent's intention and becomes the product of human interactions, the flow of adjustments and temporal constraints (Wright Mills, 1966). Without being the fruit of a single actor, the agency is the result or attribute of a network of given actors. It comprises the result of recursive events that interact. It is sometimes influenced by the social environment, coloniality. The coloniality refers to an approach that questions the structures of power and thought inherited from colonialism (Fanon, 1961). Decolonial approaches intervene at this level to understand the subject/structure relationship, which is sometimes explained through colonial thought patterns that characterise the social environment.

In this chapter, the agency measures the influence of norms and structures of thought or power in the role of CSOs in the field of electronic surveillance. It looks at the extent to which CSOs are free to act. For Hobbes, the freedom to act is only realised in situations where there are no obstacles, shackles or imprisonment (Hobbes, 2000). In this sense, anything that is not determined to act by any external cause should be called free (Bugeme, 2020). In the DRC, the public authorities restrict civil society initiatives by adopting restrictive legislation. This contributes to the restriction of civic space.

Faced with such restrictions, CSOs often adopt resilience strategies that run counter to public policy. They develop practices that fall outside the law. They are described as practices that are subversive of social laws. Their actions can be explained in part by the margins of choice and the degree to which their interests or those of the population are affected. In 2020, for example, all the CSOs protested against the public policies introducing the RAM tax, to the point of getting the government to back down. Without being contradictory in itself, this situation can be explained by the agency. In social sciences, the agency is used to explain social construction. As such, it becomes not the fruit of the will of a single actor, but the result of recursive events. The combination of these different events makes it possible to explain the social phenomenon.

Organisation and functioning of civil society: A justifying factor for the lack of interest in public monitoring of surveillance?

According to the civil society coordinator in South Kivu, 'there is no specific CSO activity in the area of electronic surveillance. CSOs only intervene when networks are disrupted or tariffs are overcharged. That's when CSOs get organised to make demands.'[1] This statement raises the question of the reasons for this lack of interest. To answer this question, the paper focuses on the organisation and functioning of civil society. The aim is to ascertain whether the organisation and operation of civil society are a factor in explaining this lack of interest.

[1] Source: Interview with NB, 12 July 2024.

Civil society is an umbrella organisation for not-for-profit associations whose legal status is based on Law No. 004–2001 on 20 July 2001, laying down general provisions applicable to not-for-profit associations and public-utility establishments. According to a more traditional definition, it includes all the organised forces in society outside the state, the family, political parties and the market. These are forces and structures such as associations, NGOs, the press, trade unions, churches and academics (Abega, 2009). In South Kivu, for example, the organisation of civil society is based on the South Kivu Civil Society Charter and the internal regulations. According to article 1er of the Charter, civil society is understood to be a grouping of structures and associations coordinated and organised at different levels of service for the vital interests of the people. It does so collectively or through the specialised mechanisms of its components.

In organisational terms, the diversity of associations makes it difficult to clearly identify the components of civil society. This difficulty can be explained by the diversity of the social-mobilisation framework, characterised by the nature of the actors (media, private institutions), the area of intervention (urban or rural) and the mobilising issues (Abega, 2009). Despite this difficulty, the doctrine classifies organisations into several components (Yamba Yamba, 1998). These include cooperative associations, cultural and sports associations, free and independent press associations, student associations, women's associations, humanitarian and philanthropic associations, learned and scientific associations, corporations, professional orders and associations, churches, youth movements, human-rights NGOs, development NGOs, employers' unions and workers' unions (Bugeme, 2020).

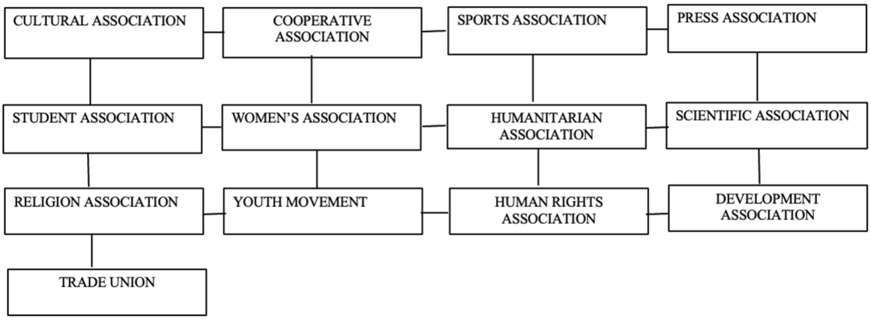

Figure 4.1: Composition of civil society in South Kivu. © Author.

This figure shows the diverse composition of civil society in South Kivu. The CSOs are diverse and varied. They pursue various objectives ranging from the protection of women's rights to religious associations. Given the diversity that makes up civil society, there are some coordination problems.

In terms of how it operates, the components of civil society come together in networks or thematic groups in order to frame their aspirations and strengthen their ambitions. In South Kivu civil society has 26 thematic groups, including Mining, Democracy and Elections, and Human Rights. Alongside the thematic groups, operational networks are emerging. In South Kivu, there are currently two major operational networks that act like NGOs in their own right, because they negotiate and receive funding while carrying out actions (Bugeme, 2020). These are the Conseil Régional Des Organisations Non Gouvernementales de Développement (CRONGD) and the Réseau des Associations des Droits de l'Homme du Sud-Kivu (RHADOSKI).

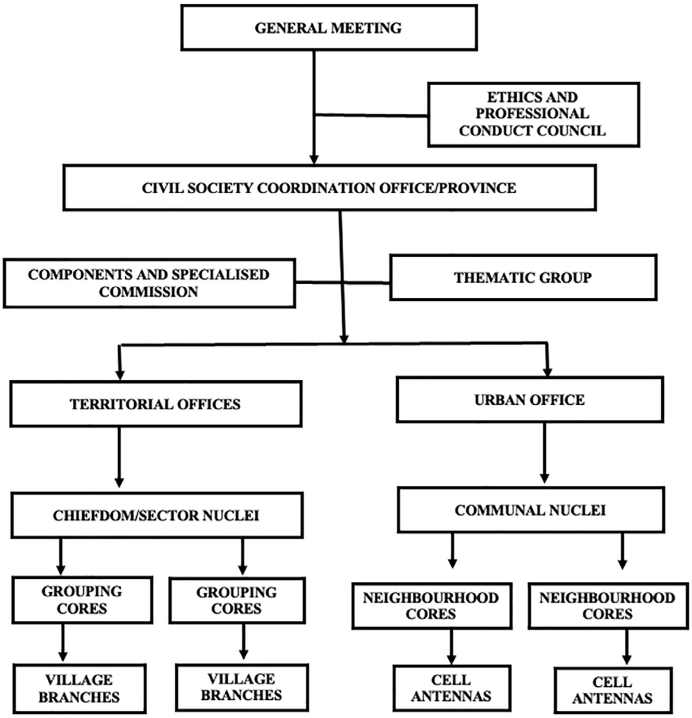

Figure 4.2: The organisation and functioning of civil society in South Kivu. © Author.

The figure above summarises the organisation and functioning of civil society in South Kivu. The organisational structure of civil society is characterised by a certain hierarchy, but CSOs act independently. At the top is the General Assembly, which brings together all the organisations that make up civil society. It is the plenary body responsible for giving broad guidelines and appointing the members of the coordination bureau. The office is responsible for coordinating the activities of all the components, although the CSOs retain their independence. The coordination office is represented in all the administrative subdivisions of South Kivu province. The aim is to ensure that civil society is represented in all parts of the province, including the remotest corners such as villages.

Based on this organisational structure, two observations can be made regarding public control of electronic surveillance in the DRC.

Firstly, there are almost no civil society organisations working in the field of electronic surveillance. In South Kivu there is only one organisation working in this field. This is the Partnership for Integrated Protection (PPI), which works in three areas: (1) documenting and preventing the control of information during the electoral period in the Democratic Republic of Congo; (2) training in digital security; and (3) setting up an online assistance platform on digital security. However, in the DRC, CSOs face restrictions on online civic space by government authorities. These restrictions are based on digital-network security and claims to digital sovereignty. The DRC government wishes to exercise control over digital activities. In the National Digital Plan, the President of the Republic expresses his desire 'to consolidate digital sovereignty' (DRC, 2019, p. 120). State services restrict civic space by resorting either to electronic surveillance of citizens or to internet control. This control is achieved by cutting off the internet, excluding people from the domain and refusing to liberalise the internet.

Secondly, there is no place in the civil society organisation chart for public monitoring of electronic surveillance. There are no components or thematic groups interested in these issues. This lack of interest is partly due to the absence of players in this field. However, public control of electronic surveillance is included in the activities of two thematic groups, namely Democracy and Human

Rights. Electronic surveillance sometimes involves restrictions on civic and democratic space. It also leads to the manipulation of personal data, which constitutes a violation of privacy. As such, CSOs should deal with it within existing thematic groups without having to create new structures. Faced with this situation, and with the advent of decentralisation, Congolese legislators are trying to put civil society back at the heart of security issues and electronic surveillance.

In 2013, the legislature adopted decree no. 13/041 on 16 September 2013 on the creation, organisation and operation of local community safety councils. The law invests these councils with two main missions. On the one hand, it seeks comprehensive and sustainable solutions to problems of public safety, tranquillity and health, within the jurisdiction of the ETDs (art. 3). This involves implementing the local community safety plan. They are also involved in monitoring and evaluating the annual or multiannual community safety plan (art. 4). Given that electronic surveillance is one of the key security issues, there was reason to be hopeful. The Council is made up of a number of leading figures, including public authorities and CSOs. Such a composition brings the security services closer to the local population for whom they have been invested. With the participation of CSOs in such local structures, the protection of the local population should be at the heart of the security services. However, the implementation of this structure is struggling. Local community security councils do not operate throughout the DRC, owing to a lack of political will (Hoebeke et al., 2019). Their establishment is therefore conditional on the adoption of the Prime Minister's decree setting out the terms and conditions of their organisation.

In 2023, the legislature adopted Ordinance-Law No. 23/010 of 13 March 2023 on the Digital Code. Article 262 of the law created a Data Protection Authority (DPA). The legislator assigns it to the main task of monitoring compliance with the protection of personal data (art. 263). The Data Protection Authority is made up of three bodies. These are the Plenary Assembly, the Bureau and the standing committees (art. 264). In the composition of this body, the legislator reserves two places out of nine to two components of civil society, including the bar and the representative of employers' organisations (art. 266). However, this structure, like the previous one, is still awaiting the Prime Minister's decree setting out the organisation and operation of the DPA. Despite the forthcoming decree, the authority's scope of action remains limited because the future ordinance will not be able to take account of personal data controlled by the security services.

Three case studies: An illustration of civil society's lack of coordination

Most of our respondents said that CSOs undertake very little action in relation to electronic surveillance. According to NB, 'There are no specific activities in this area except when there are network disruptions or overcharging, which is when civil society gets organized to make demands and find out what is going on.'[2] As for NA, 'There are no general joint actions, but there are certain associations that organise in-house training to detect whether we are being monitored and the practices and tricks that we can put in place to escape control.'[3] However, the absence of coordinated action should not detract from the existence of electronic surveillance carried out by state services. According to NA, 'public authorities and socio-political actors are tracked and sometimes geo-located.'[4] Faced with this difficulty, this section examines cases in which the authorities have resorted to electronic surveillance. The aim is to analyse the actions of CSOs against such measures.

To illustrate the role of CSOs in monitoring surveillance, the presentation focuses on three case studies. The aim is to analyse them in order to understand the actions of civil society in the face of the phenomenon of surveillance. This study attempts to understand the low interest of civil society organisations in electronic surveillance through the behaviour of the actors.

[2] Source: Interview with NB, 12 July 2024.

[3] Source: Interview with NA, 11 July 2024.

[4] Source: Interview with NA, 11 July 2024.

RAM case

In 2020, the Autorité de Régulation des Postes et Télécommunications (ARPTC) decided to levy the Mobile Appliance Register (RAM) tax. This government has several objectives. Firstly, it justifies the levying of this tax by its concern to combat the circulation of counterfeit telephones. Secondly, it is intended to combat the theft and counterfeiting of mobile terminals. Finally, through this tax, the government wants to protect the health of users against the toxic effects of devices that do not comply with local and international standards, and to increase the security and quality of service of mobile networks in DR Congo. CSOs have never been convinced by this argument, as one respondent told.[5]

In 2022, the CSOs demanded that the Congolese government abolish the RAM tax and reimburse the deductions made between September 2020 and February 2022. They took several steps.

Firstly, they are taking criminal action against the government's decision. The Comité Laïc de Coordination (CLC), a group with close ties to the Catholic Church, is bringing a civil action against the four telecommunications companies in a criminal trial. It accused them of having taken millions of dollars from their subscribers' mobile phones between September 2020 and February 2022 through a fee of between $1 and $7 per year. According to the NA investigator, this decision constitutes fraudulent misappropriation of sums belonging to others. This is an offence of theft under the Congolese Criminal Code.[6]

Secondly, the CSOs are organising public demonstrations alleging that the RAM tax is illegal. They base their argument on the constitutional principle of the legality of taxes. In the DRC there are no legislative texts instituting this tax. It is a government initiative in violation of the Constitution. In addition, the CSOs note the effects of nonpayment of the RAM tax. In the event of nonpayment, mobile-phone owners run the risk of disconnection or blocking of the network to millions of young people and women whose cost of living

[5] Source: Interview with NB, 12 July 2024.

[6] Source: Interview with NA, 11 July 2024.

remains low. To force the government to withdraw its decision, 'CSOs are organising sit-ins at all telecom companies to demonstrate their refusal to pay the RAM tax levied by them.'[7] All these actions are supported by the media through reports and radio broadcasts.[8]

Thirdly, the CSOs are carrying out systematic monitoring of the RAM dossier. The coordination office is leading this monitoring through the South Kivu consumers' league (Licoski). They are able to put a figure on the losses incurred by the inhabitants of South Kivu as a result of the RAM tax.[9] According to one respondent, thanks to the work of CSOs in South Kivu, parliamentarians have taken up the issue by questioning the Minister for New Information Technologies. Not only was the tax illegal, but several million dollars had been misappropriated.[10] Failing to pass a motion of no confidence in the minister, the government abolished the RAM tax in March 2022 following strong pressure from CSOs.

The decision to withdraw the RAM tax was based more on relieving the tax burden than on electronic surveillance. In this case, the government demonstrated its ability to access any subscriber's phone and disconnect it at any time, either globally or in a targeted manner. This enables it to manipulate the personal data of millions of subscribers. The technology used to collect tax enabled the government to restrict access to certain mobile-phone functions. According to one interviewee, the government is proving that it can access every subscriber's phone. It can also disconnect them at any time globally or in a targeted manner. Millions of Congolese were surprised to see their access to certain functions of their mobile phones restricted because they had not paid this illegal tax.

In addition to disconnecting SIM cards from the network, the government acknowledged during a parliamentary hearing with the Minister of New Information Technologies that 'RAM offers solutions that, in collaboration with the security services, can combat kidnapping and other crimes through the geolocation of mobile

[7] Source: Interview with CM, 17 July 2024.

[8] Source: Interview with PM, 19 July 2024.

[9] Source: Interview with NA, 11 July 2024.

[10] Source: Interview with NB, 12 July 2024.

devices.'[11] Geolocation makes it possible to indicate 'the geographical position of the terminal equipment of a user of an electronic communications service' (Directive 2002/58/EC OF THE EUROPEAN PARLIAMENT). It allows the movements of an individual to be tracked in real time or their presence at a given location to be verified. On phones, geolocation can use three techniques: 'First, a mobile phone can be "pinned", i.e., identified by the nearest base station that identifies its signal. Secondly, the interface may use a satellite geolocation service, such as GPS (Global Positioning System). Thirdly and finally, Wi-Fi technology can also be used to locate an interface' (David Lefranc, Droit des applications connectées – Applications – réseau – interfaces, Larcier, Brussels, 2017, § 994). According to an employee of a telecommunications company, 'the government can use the IMEI number to link communications to a specific device, which will facilitate both the interception of communications and geolocation'.[12]

Faced with this situation, CSOs expressed fears that the government would use this technology to block all critical voices or control citizens' communications.[13] Their actions helped influence the public policies implemented by the government. Indeed, when the Digital Code was adopted in 2023, it limited the use of geolocation and wiretapping. Articles 186 et seq. of Ordinance-Law No. 23/010 on the digital code stipulate that all processing of personal data must be declared to, or authorised by, the Data Protection Authority, failing which it is unlawful. However, intelligence services are not affected by this restriction because the Digital Code does not apply to such structures.

[11] Response from His Excellency Augustin KIBASSA MALIBA, Minister of Posts, Telecommunications and New Communication Technologies, to the oral question with debate on the Mobile Device Register (RAM) asked in the National Assembly by the Honourable MISARE MUGOMBERWA Claude, available at https://lesvolcansnews.net/2021/10/14/affaire-ram-integralite-de-la-reponse-du-ministre-des-pt-ntic-aux-deputes-nationaux/.

[12] Source: interview with CT, 15 July 2024.

[13] Source: interview with NB, 12 July 2024.

Heri Kalemaza case

The tribunal de grande d'instance de Bukavu prosecuted Heri Kalemaza for attempting to undermine the honour and reputation of the provincial governor of South Kivu. The prosecutor accused him of having defamed the governor of South Kivu in the WhatsApp group 'Unis par le droit/ UOB'. He is accused of several acts. Firstly, the defendant accused him of embezzling 3,5000,000 dollars borrowed from the RAWBANK bank. Secondly, the defendant alleged that the governor hacked into the accounts of the province of South Kivu in order to organise an unspeakable tax evasion (Tribunal de paix de Bukavu, 2020).

In judgment RP 3386/ III of 30 September 2020, the Tribunal de Paix sentenced him to a fine of 250,000 Congolese francs for the offence of defamation. The Court based its decision on the act of imputation and the publicity required to commit such an offence. With regard to the act of the imputation, the Court held that the defendant had published these facts 'in the WhatsApp group "Unis par le droit/ UOB", on 26/12/2019, 27/01/2020 and January 2020 respectively' (Bukavu Peace Court, 2020). With regard to the act of publicity, the Court based its reasoning on the defendant's writing broadcast in public in the same WhatsApp group 'Unis par le droit/ UOB'. According to the Court, 'although it is a virtual environment, the WhatsApp group is accessible to 70 interactive people. It is certain that more than one of them read these messages. These kinds of digital platforms are eminently public, which is why they are called social networks' (Tribunal de paix de Bukavu, 2020).

Ultimately, the Court convicted the defendant without demonstrating how he accessed the content of the WhatsApp messaging service. Given that this messaging system is protected by encryption, access to the content can be explained in several ways. First, access to the content may be justified by the composition of his group. Heri Kalemaza was part of a WhatsApp group composed of several people. Some of them allegedly collected the data and passed it on to the provincial authorities. Secondly, access to the content was the result of surveillance carried out by the intelligence services. According to the person concerned, 'there is nothing to rule out the possibility that ANR agents joined the WhatsApp group using false identities to intercept communications'. The context at the time was conducive to this, as the case comes at a time when 'dozens of people who have criticised government policies, particularly on social media, have been subjected to intimidation and threats, beatings, arrests and, in some cases, prosecution' (Human Rights Watch DR Congo, 2020). There is strong pressure on opponents through the strengthening of surveillance and surveillance capabilities at the level of state structures. According to the CIPESA NGO report, 'Congolese government bodies have, in the past, made requests to telecommunications companies to intercept communications or disclose customer data (…). Sometimes, political authorities do not need to go through official channels for personal interests. For example, it has been reported that President Kabila hired an Israeli company, Black Cube, in June 2019 because he wanted to know everything about his political opponents, but also about his own troops, where traitors might be hiding. Israeli intelligence agents are said to have taken up residence at the Grand Hotel in Kinshasa to carry out, among other things, telephone tapping – an allegation they have denied' (CIPESA, State of Internet Freedoms in the DRC 2019 – Mapping trends in government control of the internet, 1999–2019, January 2020, p. 12).

Through such acts, the government is restricting digital civic space by affecting online democracy. This limits freedom of expression, leading CSOs to censor themselves. The government controls digital space without the need for electronic surveillance.

Unlike the RAM case, the case of Heri Kalemaza did not provoke a strong mobilisation of CSOs. In an interview, a respondent criticised the variable geometry of CSO involvement in Bukavu.[14] There are several explanations for this situation.

The first explanation lies in the political nature of the dispute. One respondent explained the situation as follows:

> There was no strong mobilisation around the Heri Kalemaza case. This is one of the weaknesses of the CSOs in Bukavu.

[14] Source: Interview with HK, 15 July 2024.

> The reason is as follows. Heri Kalemaza wore a political hat. He was a member of the Congolese Party for Progress (PCP). As such, he could not benefit from CSO support because he did not fall within the code of human rights defenders who must be accompanied in such cases. I did not agree with this approach (...).[15]

It is clear that both the victim and the accused are members of political parties. The second explanation lies in the issue of human rights. According to one interviewee, 'human rights is an issue reserved for the elite of society. The rest of the population is not concerned'.[16] As long as the arrest of an individual in violation of his or her rights does not affect the interests of the entire population, CSOs are not prepared to take up the cause. It is an isolated case with no impact on the household basket, as was the case in the RAM affair.

Despite this low level of support, the Court upheld the minimum sentence following pressure from some sections of society. He regained his freedom after conviction because the length of the sentence was equivalent to the number of days spent in detention. This logic was also followed in the Stanislas Bujakera case.

Stanislas Bujakera case

In the case of Stanislas Bujakera, the Kinshasa/Gombe High Court sentenced the correspondent of the magazine *Jeune Afrique* on 18 March 2024 to six months' imprisonment and a fine of 1 million Congolese francs. The court accused him of having committed 'forgery', 'forgery of documents', 'use of forgeries', 'propagation of false rumours' and 'transmission of an erroneous message'. He is charged with having shared a false document from the Internal Security Department of the National Intelligence Agency (ANR) in a WhatsApp group on 3 September 2023. The charge was based

[15] Source: Interview with NA, 11 July 2024.

[16] Source: Interview with HK, 15 July 2024.

on a digital analysis of the metadata. He was accused of transmitting false messages via a computer system. The Congolese state was prosecuting him for sending the false message about the investigation into the death of Mr Cherubin Okende via a fabricated ANR report to the WhatsApp accounts of individuals clearly identified in the judgment (10th page). The Congolese state used surveillance software to detect these transmissions.

The court based its conviction on several reports demonstrating that 'thanks to the MD-NEXT used via Kali Linux 22; 01.lts, the number +243823327460 used by the defendant BUJAKERA was identified through the Internet Protocol address (public IP address): 192.162.12.04, as being the first distributor of this fabricated report on WhatsApp, and that the experts traced the numbers attached to clearly identified recipients' (26th page). Consequently, the Court found 'this charge established in fact and in law and sentences him to six months (6 months) of principal penal servitude' (26th page).

For its part, the journalist's defence team demonstrated that such an analysis was unfounded for technical reasons. Indeed, there was no evidence that this address was used by the journalist's phone. The IP address in question was assigned to a web server located in Spain. The Telegram and WhatsApp platforms from which the message was allegedly sent did not allow messages to be traced or metadata to be stored that would enable them to be identified (Kinshasa/Gombe High Court, 2024).

In the DRC, as in many countries, states use technological and digital advances to carry out preventive surveillance in the name of national security in general and, in particular, in the name of the fight against terrorism (https://www.radiookapi.net/2024/02/24/actualite/justice/felixtshisekedi-jai-decide-de-me-meler-du-dossier-de-larrestation-du).

In countries with 'authoritarian' governance such as the DRC, digital surveillance serves as both a repressive and a destructive lever for those in power. With the advent of the Digital Code, the legislature established the National Cybersecurity Agency, entrusting it with several missions (Digital Code, Articles 275 to 280). From now on, this agency will intercept not only personal data but also, and above all, citizens' conversations (AE, A. E., TP, T. I., &amp; Ritimo

(2020) DRC Protection Programme: Country Profile on Digital Security). In most cases, these practices are justified on grounds of national security.

In this case, journalist Stanislas Bujakera was subject to double surveillance of his telephone conversations. Prior to this, the defendant was subject to electronic surveillance of his conversations by the ANR. When he was arrested at Ndjili airport by the ANR, the authorities accused him of transmitting false messages and spreading false rumours (p. 12). Such accusations can only be based on increased surveillance by the authorities. Subsequently, the court ordered that his various conversations be examined by independent experts in order to establish the truth. However, these government interferences are contrary to freedom of expression (Const. Art. 23) and privacy (Const. Art. 31). As the guarantor of freedoms, the judge should have examined the proportionality of such surveillance measures. Instead, he convicted the defendant on grounds that raise a number of questions.

In his reasoning, the judge referred to the IP address to attribute the transmission of the message to the defendant's telephone. According to the court, 'the number used by the defendant BUJAKERA was identified through the Internet Protocol address' (p. 26). This reasoning raises the question of the role of the IP (Internet Protocol) address in electronic surveillance. The IP address is a unique identifier for any device connected to the internet (a computer, smartphone, tablet or any other connected device). Each device is assigned an IP address that uniquely identifies it and allows it to communicate with other devices on the internet. IP addresses play several roles, including user identification, online activity tracking, access blocking, criminal investigations, government surveillance and so on.

However, when it comes to electronic surveillance, it does not apply to applications that use end-to-end encryption. Several messaging applications have integrated this technology to ensure a level of confidentiality. This is the case with Signal, WhatsApp and Telegram. Through the end-to-end encryption used by these devices, data is exchanged directly between end users without passing through a centralised server. In this case, the IP addresses of the devices involved in the communication were used to route the data directly between them, without passing through an intermediate server. The purpose of encryption is precisely to solve the problem at its root by not allowing the server to read everything between senders and recipients. The message remains encrypted from one end (the sender) to the other (the recipient), without ever being decrypted between the two points, hence its name. This technique offers users several advantages, including increased confidentiality, protection against data leaks, reduced risk of espionage, data integrity, protection against government requests, increased user confidence, privacy protection and so on.

Given this end-to-end encryption, in this particular case, the government could not identify Stanislas Bujakera as the author of the message. Technically, this was therefore impossible. This case highlights the difficulty for judges to protect fundamental rights in the face of security imperatives. In such a context, the government carries out electronic surveillance of citizens without the judge being able to stop or control it. Once such intrusions are provided for by law and justified on security grounds, the judge should examine them in the light of the principle of proportionality. Otherwise, he sacrifices fundamental rights on the altar of security imperatives.

Although most of the people we interviewed in South Kivu were not familiar with this case, it had been the subject of strong mobilisation by CSOs in the DRC, particularly the 'Press and Media' component.

Initially, the international press were very active. All the organisations that defend journalists were mobilised around this issue. Reporters Without Borders (RSF) devoted an investigation to the case.[17] According to an interview with a journalist, 'this strong mobilization can be explained by the fact that the journalist worked for an international media, namely Jeune Afrique. The response would

[17] RSF investigation. Stanis Bujakera case in the DRC: the journalist is not the author of the note for which he is facing 10 years in prison, available at https://rsf.org/fr/enquête-rsf-affaire-stanis-bujakera-en-rdc-le-journaliste-n-est-pas-l-auteur-de-la-note-pour

not have been the same if it had been a journalist working locally.'[18] At every press conference abroad, the Head of State had to answer a question about this affair. In an interview with RFI and France 24 on 16 November 2023, the President of the Republic said the following: 'I am neither behind his arrest nor pulling the strings so that he can be brought to justice. I cannot intervene,' Félix Tshisekedi replied to journalists Marc Perelman and Christophe Boisbouvier. 'I will only intervene later, perhaps, if he is convicted, for an amnesty, a pardon or whatever. But at this stage, I have nothing to say.'

Secondly, the local media mobilised alongside their international partners through the #FreeStanis campaign and the organisation of public events. At a special press briefing in Kinshasa with the Minister of Communication on 22 February 2024, the President decided to get involved in the case, saying: 'Journalist Stanis Bujakera may be a victim of the dysfunction of the Congolese justice system,' and promising that on Saturday, 22 February he would inquire about his case with the justice system, which he described as 'sick'.[19]

Thanks to this strong mobilisation, the authorities had to change their perception of Stanislas's case to the point of influencing the Court's decision in such a way that he was released despite the conviction. Instead of releasing him, the authorities sentenced him to six months' imprisonment. However, he had already served his sentence. The sentence was therefore equivalent to an acquittal. It is not clear what impact this case will have on electronic surveillance.[20] Although the CSOs obtained the release of their colleague, they never asked for the law authorising the ANR to carry out electronic surveillance to be amended.

Beyond the strong mobilisation of CSOs, this case raises the question of the role of the IP (Internet Protocol) address in electronic surveillance. According to one interviewee, the IP address is a unique

[18] Source: Interview with PM, 19 July 2024

[19] Radio Okapi, 23/2/2024 https://www.radiookapi.net/2024/02/24/actualite/justice/felixtshisekedi-jai-decide-de-me-meler-du-dossier-de-larrestation-du).

[20] Source: interview with P.M., 19 July 2024

identification tool for any device connected to the internet (a computer, smartphone, tablet or any other connected object). Each device is assigned an IP address that uniquely identifies it and enables it to communicate with other devices on the internet. The IP address plays a number of roles, including identifying users, monitoring online activities, blocking access, criminal investigations and government surveillance.[21]

However, electronic surveillance does not apply to applications using end-to-end encryption. Several messaging applications have integrated this technology to ensure a level of confidentiality. These include Signal, WhatsApp and Telegram. Through the end-to-end encryption used by these devices, data is exchanged directly between end users without passing through a centralised server. In this case, the IP addresses of the devices taking part in the communication are used to route the data directly between them, without going through an intermediary server. The aim of encryption is precisely to solve the root of the problem by not allowing the server to read everything between sender and recipient. The message remains encrypted from one end (the sender) to the other (the recipient), without ever being decrypted between the two points, hence its name. This technique offers users a number of advantages, including increased confidentiality, protection against data leaks, reduced risk of espionage, data integrity, protection against government requests, increased user confidence and protection of privacy.[22]

Given this end-to-end encryption, the government could not identify Stanislas Bujakera as the author of the offending message. Technically, this was impossible unless the sender used a VPM that dynamically assigned IP addresses. The court did not demonstrate this.

In view of the above, the mobilisation of CSOs is mixed and varies from one case to another. The presentation will now focus on the factors that explain such actions. The aim is to understand the reasons for this variable-geometry mobilisation of CSOs in the face of cases of electronic surveillance.

[21] Source: Interview with C.M., 17 July 2024.

[22] Source: Interview with C. M., 17 July 2024.

Factors explaining the low mobilisation of CSOs

In the DRC, the future of digital freedoms is at the heart of the news. Citizens are faced with contradictory situations. The exercise of their digital freedoms contrasts with policies aimed at narrowing the space for online freedoms. Over the past few years in several Central African countries, and particularly in the DRC, the future of digital freedoms has been at the heart of the news, especially where liberal democracies are concerned (information sharing, free expression, calls for uprisings and so on). On the one hand, internet users are faced with situations that at first sight seem contradictory, characterised by the availability of online solutions and, on the other, the strengthening of a balance of power that is increasingly unfavourable to public freedoms. On the one hand, there are emerging aspirations to benefit from certain digital freedoms. On the other, there are government strategies to regulate online activities.

However, CSOs exert little or no pressure on these new forms of restriction of civic space and digital democracy. The case studies demonstrate this. There is little or variable mobilisation on the part of CSOs. During the interviews, the interviewees identified the strengths and weaknesses of CSO mobilisation. These are endogenous and exogenous causes. The aim of the presentation is to elucidate their scope.

Endogenous factors

There are a number of reasons for the low level of CSO involvement in the government's electronic surveillance.

Firstly, the lack of motivational commitment on the part of the population justifies the low level of mobilisation of CSOs. According to one interviewee, 'human rights violations and electronic surveillance only concern the elite of the Congolese population. As long as the population as a whole is not affected by public policies, the mobilization of CSOs will remain lacklustre'.[23] In the RAM case, CSOs mobilised because all telephone holders were subject to the RAM

[23] Source: Interview with HK, 15 July 2024.

tax without discrimination. Unlike the RAM case, CSOs did not take up the cause of the Heri Kalemaza case, which was considered to be an isolated conflict between political players. This situation can be explained by the agency theory. According to this theory, the causes of action lie in the actor's intention (Davidson, 1980). Intention implies the actor's motivation, which must be proportional to the interests involved. The theory of affected interests, a variant of the agency, provides a better explanation for this low level of mobilisation. According to this theory, membership of a state political community presupposes the existence of common interests that may be affected by a national decision (Beckman, 2006). Used to exclude foreigners from exercising their political rights, this theory explains the low level of mobilisation of CSOs. CSOs can only be mobilised if the interests of the population are affected by public policy. La Fontaine's famous maxim is eloquent: *'ILS NE MOURAIENT PAS TOUS, MAIS TOUS ÉTAIENT FRAPPÉS'* (La Fontaine, 1678–79). If they are not all struck down, public control of surveillance will remain a pious hope.

Secondly, the organisational structure of CSOs in South Kivu also explains this low level of mobilisation. According to one interviewee, 'there is no thematic group within civil society devoted to electronic surveillance. Although this issue could be included in existing themes such as democracy or human rights, CSOs are not equipped.'[24] However, their membership of this thematic group contributes to CSO capacity building. The latter is defined as a deliberate process that increases the capacity of an individual, group, organisation, network or system to improve or develop new knowledge, skills, attitudes (KSAs), systems and structures needed to function effectively, work towards sustainable development and achieve goals (CRS, 2017). CSOs understand capacity building as 'a training package' or 'upgrading actors'. However, there is no such training for CSOs. Another interviewee said that 'these days there are one or two organisations that train CSOs to protect themselves against electronic surveillance techniques'. CSOs do not have a holistic approach to this problem. This is a weakness on their part. Thus, in

[24] Source: Interview with NB, 12 July 2024.

the RAM case, although the mobilisation was a success, the CSOs reduced their actions to withdrawing the tax without demanding an end to the monitoring of telephones by state services. This situation can be explained in terms of agency. An individual's actions are influenced by the environment. Faced with a social environment characterised by a lack of capacity building, there is no reason to expect mobilisation in the future.

Exogenous factors

Based on the interviews, the study identified several factors that are not directly related to CSOs. One interviewee revealed that 'the relationship between CSOs and donors is marked by colonialism. According to him, although CSOs are described as partners by donors, they remain in a completely unequal relationship. Their relationship is tinged with coloniality. This concept[25] 'reflects the material and symbolic relationship of domination of Europe over the rest of the world' (Le Petitcorps and Desille, 2020). The aim is to see to what extent and how colonial conceptual and ideological thought patterns are reflected in a country's public policies (Spijkerboer, 2023) or in social relations. In South Kivu, coloniality is reflected both horizontally and vertically.

On a vertical level (state–individual relationship), coloniality is measured through the public policies adopted by the state. Such policies can justify the weak mobilisation of CSOs. To reduce this mobilisation, the state restricts civic space and freedoms through repressive legal texts.

In the DRC, repressive legal texts are tinged with coloniality. For example, offences against the state were imported from the colonial era and contain patterns of colonial thinking. The prohibition of subversive activities is a constituent element of several offences. It appears in Article 52 of our Constitution. According to this provision, 'All Congolese have the right to peace and security, both nationally

[25] This concept was the work of Anibal Quijano. On this subject, 1. Quijano, A. 2000. Coloniality of power and eurocentrism in Latin America. *International Sociology* 15(2), pp. 215–32.

and internationally. No individual or group of individuals may use any part of the national territory as a base for subversive or terrorist activities against the Congolese State or any other State.' Subversion, according to the common meaning of the term, is defined as 'illegal action, often covert, aimed at undermining established values and institutions' (Rey-Debove and Rey, 2015). Such vague incriminations restrict civic space and contribute to limiting the actions of CSOs.

In 2023, the government adopted the Digital Code, which made it a criminal offence to spread false rumours on the internet. The people interviewed welcomed the initiative of this law. One civil society player 'welcomes the adoption of the Digital Code. This law has not been sufficiently publicised. As a result, many people don't know about it'. However, the process that led to the adoption of this law deserves to be criticised in terms of both form and content.

In terms of form, the power to adopt the Digital Code falls within the remit of the law under Article 122 of the Constitution.[26] The legislator has exclusive powers in this area, which is not a concurrent matter. The government cannot intervene in the area of the law without the authorisation of Parliament. With regard to the Digital Code, the President of the Republic relies on Article 129 of the Constitution.[27] This provision authorises the National Assembly to grant the government the power to legislate, during the parliamentary recess, in place of the National Assembly. On the basis of this authorisation, the government adopted the Digital Code. Ultimately, this code was adopted in the DRC without being examined by the people's representatives. It is a law that has no legitimacy. On a

[26] Article 122 of the Constitution: 'Without prejudice to the other provisions of this Constitution, the law shall lay down rules concerning: (...) 6. the determination of offences and the penalties applicable thereto, criminal procedure, the organisation and functioning of the judiciary, the creation of new orders of courts, the status of magistrates, the legal regime of the Supreme Council of the Judiciary; (...).'

[27] Art. 129 of the Constitution: 'The Government may, for the urgent execution of its programme of action, ask the National Assembly or the Senate for authorisation to take, by ordinance-laws, for a limited period and on specified matters, measures which normally fall within the domain of the law.'7

substantive level, the digital code excludes the security services from its scope. The latter carry out electronic surveillance without their actions being monitored.

During the colonial era, the administration controlled the indigenous population in order to protect colonial power by adopting repressive legislation. Today, public policy reflects the same pattern. The administration is restricting space by using the same methods as the coloniser. The DRC should follow the example of Kenya, where the judge in the Joshua Ayika case challenged this way of thinking.

The courts are prosecuting a civil society activist for publishing on X (formerly Twitter) the possibility of the army taking control of the government for 90 days. The post was made during a period of public protests against the high cost of living. As a result, he was prosecuted in Kenya's High Court. The person concerned, Joshua Ayika, posted on X (formerly Twitter) that the army could take control of the government for 90 days. Joshua made the post during protests against the high cost of living led by opposition parties. After acquitting him, the court annulled article 77 (1)(a) of the Penal Code, which provides for the offence of subversive activities. The judge's objective was to eradicate the colonial legacy in Kenya's legal system. According to the Court:

> 105. It is not far from our lips and eyes that independent Kenya inherited from the colonial state a repressive system . . . 135. It therefore goes without saying that, Section 77(1) and (3) of the penal code is a colonial legacy which limits freedom of expression through the vaguely worded offence of subversion (Malidzo Nyawa, 2024, § 105).

By striking down this subversion provision of the Kenyan Penal Code, the Court took an important step towards eliminating the colonial legacy from the Kenyan legal system. The ruling illustrates how judges in postcolonial contexts interpret the law in light of the country's history (Malidzo Nyawa, 2024). This case reveals the colonial patterns that characterise African legislation. Like Kenya, the DRC is no exception. Such public policies influence the behaviour of actors and their agency.

Horizontally, coloniality manifests itself in the relationship between CSOs and donors. Although they are considered partners, CSOs do not receive equal treatment from donors. According to one interviewee, 'Funding is decided in the North, as is the direction it takes. Their mobilisation in the electronic surveillance sector remains limited due to a lack of funding. Nor can they redirect the funds allocated to this sector, where the stakes are so high.'[28] For this reason, another interviewee argues in favour of 'decolonizing official development assistance and access to funding'.[29] The aim is neither to revisit the colonial period nor to oppose one vision to another, but rather to study the challenges of the contemporary world by widening the prism of analysis and agreeing to shift it. There are various approaches to decentring. It involves distancing oneself from the object of funding in order to consider it from other angles. It also means integrating into the analysis an awareness of the relationships of domination that may have defined a framework. And, of course, it means accepting that other realities, other than 'our own', deserve to be studied.

Conclusion

Towards public monitoring of electronic surveillance: a matter of time

This chapter examined the role of civil society in public scrutiny of state electronic surveillance. The results have been mixed, as the case studies have shown. This paper proposes two prerequisites for establishing public oversight of surveillance.

On the one hand, the success of public monitoring requires the establishment of an 'electronic surveillance' thematic group within civil society in the DRC. The nonexistence of such a group is a weakness linked to the organisational structure of civil society. However, such groups enable CSOs to develop networks with the

[28] Source: Interview with H.K., 15 July 2024.

[29] Source: Interview with H.K., 15 July 2024.

aim of emerging and strengthening each other (Bugeme, 2020). Following the example of the 'natural resources' thematic groups that exists in all civil societies and whose work made a major contribution to the reform of the mining code in 2018,[30] this thematic group should serve as a starting point for discussions on electronic surveillance in the DRC.

On the other hand, the future of public control of electronic surveillance depends on whether or not CSOs take ownership of certain security services. Since the start of decentralisation in 2006, public policies have included CSOs in certain security and public-protection services. In 2013, through decree no. 13/041 on 16 September 2013, the legislator created local councils for local security, with the possibility of CSOs to join as members. In 2023, the legislator set up the Data Protection Authority (DPA) in which CSOs sit as members.

Civil society should take ownership of a campaign for the establishment of such structures. Only then will public control of electronic surveillance emerge in the DRC.

References

Abega, S.C. 2009. *La société civile camerounaise et la malédiction de la Belle au bois dormant.* In: Mbonda, E-M. ed. *Annales du CERJUS P*, n°001, *La refondation de l'État en Afrique. Justice, efficacité et convivialité*. Yaoundé: Terroirs.

Abu-Laban, Y. 2014. Gendering Surveillance Studies: The Empirical and Normative Promise of Feminist Methodology. *Surveillance & Society* 13 (1), 44–56.

Albarello, L. 2001. *Choisir une étude de cas comme méthodes de recherche.* Brussels: De Boeck.

Amuli, K., Mushi, M. and Yamba Yamba, S.N. 2003. *La société civile congolaise: État de lieux et perspectives.* Brussels: Colophon.

Arendt, H. 1978. *The Life of the Mind, vol. 2.* New York: Harcourt Brace.

Beckman, L. 2006. Enfranchising Citizenship and Voting Rights: Should Resident Aliens Vote? *Citizenship Studies* 10, 152.

[30] Source: Interview with NB, 12 July 2024.

Bugeme, Z.Z. 2019–20. *Subjectivité des acteurs et conflictualité au sein des OSC en RDC: entre influence des normes et agencéité.* PhD thesis, Catholic University of Central Africa, unpublished.

Cambien, A. 2008. *Une introduction à l'approche systémique: appréhender la complexité.* Rapport de recherche, Centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques (CERTU).

Camila P., 2020. Rendre visibles les conséquences de la surveillance numérique Le cas du scandale Cambridge Analytica, Open Edition Journals vol. 37/2 | 2020 (https://journals.openedition.org/communication/13252).

Cappelle, J. and Custers, R. 2009. *Rechercher la problématique des ressources naturelles dans la République Démocratique du Congo.* Antwerp: IPIS vzw.

Castagnino, F. 2018. Critique des surveillance studies. Éléments pour une sociologie de la surveillance *Déviance et Société.* 42(1), pp. 9–40. [Online]. Available from: https://doi.org/10.3917/ds.421.0009.

CERDHO. 2022. *Bonne gouvernance des Ressources naturelles, Droits de la personne et Développement communautaire en République démocratique du Congo: Analyse diagnostique de base contextuelle et organisationnelle.* Report, July 2022.

CORNUT ST-PIERRE, 2019. « Utilisations et finalités des registres du commerce à l'ère numérique : de l'efficacité économique à la surveillance citoyenne des entreprises. » Les Cahiers de Droit, vol. 60, n° 3 : 589-622.

Davidson, D. 1980. *Essays on Action and Events.* Oxford: Oxford University Press.

De Sardan, O. 1995. Anthropologie et développement : Essai en socio-anthropologie du changement social, Paris, APAD-Karthala, coll Hommes et sociétés

De Sardan, O. 2008. *La rigueur du qualitatif – les contraintes empiriques de l'interprétation socioanthropologique.* Louvain-la-Neuve: Academia Brylant.

Donnadieu, G. and Karsky, M. 2002. *La systémique, penser et agir dans la complexité.* Paris: Éditions Liaisons.

DRC. 2019. *Plan national du numérique – horizon 2025.* Kinshasa: Democratic Republic of Congo. Accessed September 2019. 120. https://presidence.cd/uploads/files/Presentation%20PNN_03_final.pdf

Fanon, F. 1961. *Les damnés de la terre.* Éditions Maspero

Goodman, R., ed. 1995. *Pragmatism.* London: Routledge.

Hobbes, T. 2000. *Le léviathan.* Paris: Gallimard.

Hoebeke, H., Van Der Lijn, J., Glawion, T. and De Zwaan, N. 2019. *Garantir la stabilité légitime en RDC: hypothèses extérieures et perspectives locales.* Étude de politique, Stockholm International Peace Research Institute (SIPRI) and Cordaid.

Human Rights Watch. 2020. RD Congo: Restriction croissante des droits – La répression touche les médias, les détracteurs et les manifestants. *Human Rights Watch*. [Online]. Available from: https://www.hrw.org/fr/news/2020/07/22/rd-congo-restriction-croissante-des-droits.

La Fontaine, Jean de. 1678–9. *Les animaux malades de la peste, Fables.*

Le Petitcorps, C., Desille À., 2020. « La colonialité du pouvoir aujourd'hui: approches par l'étude des migrations », Migrations Société, vol. 2020/4, n°182.

Lyotard, J.F. 1991. *Phenomenology.* New York: SUNY Press.

Maheshe, T. and Mushagalusa, J.P. 2021. *Digital Surveillance and Privacy in DRC: Balancing National Security and Personal Data Protection.* Media Policy and Democracy Project.

Nyawa, M.J. 2024. Colonialisme, droit pénal et poubelle de l'histoire: On Kenya's Subversion Judgment. *VerfBlog*. [Online]. Available from: https://verfassungsblog.de/colonialism-criminal-law-and-the-dustbin-of-history/. DOI: 10.59704/916e460f0c11655b.

Plato. 1834. *La République, Livre X*, traduit par Victor Cousin. *Œuvres de Platon*. Paris: Rey et Gravier.

Quijano, A. 2000. 'Coloniality of Power and Eurocentrism in Latin America'. *International Sociology.* 15(2), 215–32.

Rebughini, P., and Colombo, E., eds. 2023. *Framing Social Theory Reassembling the Lexicon of Contemporary Social Sciences.* New York: Routledge.

Rey-Debove, J., et Rey, A. (dir.), 2015. Le Petit Robert 2014, nouvelle édition du Petit Robert, texte remanié et amplifié, Paris, Dictionnaire Le Robert, Sejer.

Salvas, B. 2001. *La protection de la vie privée sur le Web avec P3P: l'arrimage incertain du technique et du juridique.* Master's thesis in law (L.L.M.), Université de Montréal.

SetThings. [Online]. Available from: https://www.setthings.com/fr/contre-espionnage-communautes-epistemiques-en-ue/.

Sfetcu, N. 2020. Contre-espionnage – Communautés épistémiques en UE. *SetThings*. [Online]. Available from: https://www.setthings.com/fr/contre-espionnage-communautes-epistemiques-en-ue/.

Spijkerboer, T. 2023. Coloniality and Case Law on the Australian Asylum

Offshoring Scheme. *International Journal of Migration and Border Studies.* 7(2).

Tribunal de grande instance de Kinshasa/Gombe. 2024. *Judgment no. RP 29. 823, 18 March 2024, Public Prosecutor and Civil Party Théo Ngwabije Kasi against the defendant Stanislas Bujakera Tshiamala.* Unpublished.

Tribunal de paix. 2020. *Judgement No RP 3386/III, 30 September 2020, Public Prosecutor and Civil Party Théo Ngwabije Kasi against the defendant Heri Kalemaza Nicodeme.* Unpublished.

Viana, A. 2021. La surveillance numérique en temps de pandémie. *Revue internationale dedroit des donnéeset du numérique.* 7, pp. 165-78.

Vuilleumier, C. n.d. *Espionnage, police et secrets d'État.* La Cité.

Wright Mills, C. 1966. *Sociology and Pragmatism.* New York: Oxford University Press.

Interview

1. Interview with NB, 12 July 2024.

CHAPTER FIVE

Factors influencing public oversight of digital surveillance for intelligence purposes: The case of Mauritius

Sarah Chiumbu

Introduction

State surveillance has been an increasing global trend, particularly following the terrorist attacks in the United States on September 11, 2001. With the rise of digital technologies and big data, governments now possess the ability to conduct extensive, large-scale monitoring of their populations. Western governments rationalised the use of invasive monitoring by arguing the need to fight terrorism and safeguard national security (Duncan, 2022). Africa has not remained untouched by these developments. In the wake of the USA terrorist attacks, many governments across the continent adopted laws allowing them to monitor citizens' movements and intercept communications. Over the years, the proliferation of digital technologies, including Closed Circuit Television (CCTV) cameras, facial recognition systems and biometric identification tools, has facilitated the implementation of surveillance systems across the continent (Abebe, 2018; Gadzala, 2018; Brown, 2020). Apart from a few countries, there has been little accountability and oversight of these developments. Because surveillance practices have become normalised and deeply embedded, governments – both authoritarian and democratic – can now justify them (Munoriyarwa and Mare, 2022). Public oversight of surveillance for intelligence purposes is becoming increasingly important and needed to curtail surveillance overreach. Formal institutional methods for oversight are unlikely to produce substantive accountability because many African governments lack strong institutional frameworks.

In Southern Africa, there have been effective instances of public oversight; nonetheless, the nature and factors of public oversight remain little understood and have not been thoroughly examined. Mauritius is one of the few countries that act as an example of an effective and successful public oversight over the government plan in 2013 to introduce a smart ID card linked to a centralised biometric database of all personal citizen data (Duncan, 2022). A digital ID system can be viewed as a form of intelligence-driven surveillance because it involves the collection, processing and storage of personal data that may be monitored by governments or security agencies. These systems amass a wide range of information, including biometric data and activity logs, enabling the tracking and profiling of individuals in real time. The concern arises when this data is used not only for identity verification but also for covert surveillance, without individuals' consent, leading to privacy concerns. This gives states substantial control over citizens' movements and activities, akin to surveillance practices employed in security contexts (see Lyon, 2009; Walby and Hier, 2009).

The plan to introduce the digital ID in Mauritius faced opposition in the form of public protests and legal challenges. In response to the public outcry, the government suspended the project and in 2015 conducted a review of the system and updated the data protection law in 2017 to align with the European General Data Protection Regulation and the Convention for Protection of Individuals regarding automatic processing of personal data (Baichoo et al., 2018). Drawing largely from desk research, this chapter analyses the factors that influenced public oversight and the government's response to the public protest. To do this, it draws on literature on surveillance, social movements and political science to understand three factors: (1) the nature of state surveillance for intelligence purposes; (2) the socio-political conditions that contributed to the successful public oversight and (3) the political conditions under which the government suspended the biometric card and adopted progressive data-protection laws. Considering these three factors enables us to determine if Mauritius has the ideal political, socioeconomic and other conditions to serve as a best-practice model for building public oversight mechanisms in other African countries, or whether this successful public oversight was the consequence of a confluence of developments peculiar at that historical time. Strong institutions create the essential framework, accountability mechanisms and transparency that enable effective public oversight. In countries with weaker institutions, it is possible that a unique set of historical circumstances may result in successful public oversight on a one-time basis. However, this success may not be replicated in other instances when such oversight is needed.

A note on methodology

In preparation for this chapter, ethics-clearance approval was sought from the Ethical Clearance Committee University of Mauritius through a research colleague from the university. Unfortunately, the request was denied by the Committee due to the research being deemed 'sensitive'. The applicant was advised to seek approval from the Ministry of Information and Communication Technology, but this approval was referred back to the Ministry of Education, Tertiary Education, Science and Technology, which itself stated that the request had to be sent to the Prime Minister's Office, such that no approval has yet been granted to date. Consequently, without ethics approval, the planned key-informant interviews and focus-group discussions could not be conducted. As a result, this chapter relies on secondary sources for data collection. The chapter employs historical analysis as a methodological framework to explore the complexities of the past and how they shed light on current events. This approach also helps in understanding Mauritius's tradition of civic agency and public oversight. The sources of data include journal articles and books. Additionally, archival research was utilised, involving the systematic examination and analysis of archival materials to gather primary-source information on the developments surrounding the smart ID, as well as the protests and court actions related to it. Archival research was used to trace the debates over the smart ID from its introduction in 2013 to the conclusion of key strategic litigation in 2017. Sources included newspaper articles, statements from pressure groups, court rulings and parliamentary gazettes. In the absence of primary data, a literature review was also conducted to gather insights from other scholars who have written on the smart ID issue. These methods were further supported by policy analysis, where key legislation such as the Data Protection Acts of 2004 and 2017, the National Identity Card Act, and the Civil Status (Amendment) Act of 2001 were examined. This analysis provides insights into the legal and regulatory context surrounding the smart ID card.

Mauritius: Socio-economic and political context

Mauritius is an Indian Ocean Island nation in East Africa. Despite being recognised as an African nation, Mauritius differs greatly from other African nations in several significant ways. It was first inhabited by the Dutch in the seventeenth century, followed by periods of French and British colonisation (Houbert, 1981). It gained independence from Britain in 1968 and became a republic in 1992. Independence came after three decades of active political manoeuvring and negotiations rather than that of a national liberation struggle (Ramtohul, 2018). Multi-party politics was, therefore, firmly established at independence, guaranteeing political stability, social cohesion and economic diversification (Phaala, 2019; Ramtohul, 2021.) With its blend of the majoritarian Westminster model and practices of power sharing among the several ethnic groups that comprise the populace, Mauritius provides a fascinating example of a functioning democracy (Jahangeer-Chojoo, 2010). The opposition is a key component of Mauritius's political system, and the country's Constitution expressly recognises the role of opposition leader, who is given some consultative powers over specific institutional appointments (Bertelsmann Stiftung, 2024). Four parties dominate the political landscape since independence: the Mauritian Labour Party

(MLP), the Mouvement Militant Mauricien (MMM), the Mouvement Socialist Militant (MSM) and the Parti Mauricien Social Démocrate (PMSD). The MLP, founded in 1936, is a centre-left social-democratic political party. The MMM is a left-wing socialist political party, established by a group of students in the late 1960s, while the MSM, founded in 1983 by dissidents of the MMM, is also a centre-left political party (Bunwaree and Kasenally, 2005) and the PMSD is a centre-right party.

The ideological orientation of the Mauritius government is generally characterised by a blend of liberal democracy, social-welfare policies, and a market-oriented economy, reflecting a pragmatic approach to governance (Bunwaree, 2001; Bertelsmann Stiftung, 2024). The country has always been governed since its independence in 1968 by coalition governments of at least two parties. In many countries where coalition governments are the norm, political actors typically negotiate the formation of a coalition after the election. However, in Mauritius, all coalitions have been formed before the election. Parties reach an agreement in advance on a shared platform and programme, which they present to the electorate. They also agree on how key positions within the coalition will be distributed (Sithanen, 2003, pp. 2–3). Power has traditionally alternated between alliances formed by any two of the four parties, sometimes with additional smaller parties (with almost all possible combinations), leading to a relatively stable political environment (Phaala, 2019).

The last few years have, however, seen democratic backsliding in the country, according to influential observers and think tanks. Key factors contributing to this backsliding include allegations of executive overreach, where the government has been accused of undermining the independence of key institutions, such as the judiciary, electoral bodies, and anti-corruption agencies. Issues related to the surveillance of citizens, particularly through national identification systems like the smart ID card, have raised alarms about potential overreach by intelligence agencies. Additionally, the political parties 'have become extremely leader-centric, and power and decisions are concentrated, focused on big money and growing levels of cronyism' (Kasenally, 2022a, p. 5). Apart from the introduction of the biometric card in 2013, other measures have reined in civil liberties, including arrests of journalists in 2019, multiple suspensions of a commercial radio station's licence in 2020 and the political capture of key institutions including the legislature, where opposition members have been recurrently expelled, especially between 2020 and 2024. In addition, legislative proposals that pointed to the government's intentions to create a surveillance state were introduced in 2021 (Kasenally, 2022a). Notwithstanding imperfections (periodic nepotism and corruption, occasionally unstable coalitions), Mauritius's democracy has solidified to an extent unmatched in Africa (Kasenally, 2011; 2022a; 2022b).

The country is made up of diverse ethnic groups composed of the descendants of migrants who came to the island under various conditions from diverse geographical regions: France as settlers, the African continent as slaves, India as indentured labourers and China as merchants and traders (Maurer, 2015). This diversity has not led to conflicts; on the contrary, it has been beneficial to the country's democratic politics (David and Petri, 2013). Civic networking, trade unionism and social mobilisation are entrenched in Mauritius, owing to the country's history of indentured labour and rich cooperativism (Duncan, 2018; 2022). The umbrella body of non-governmental organisations (NGOs, the Mauritius Council of Social Services, estimated in 2019 that over five thousand voluntary organisations operate in the country. These trends help explain the unusual vitality of democracy in the country.[1]

The nature of state surveillance for intelligence purposes in Mauritius

There is a dearth of literature on intelligence and surveillance in Mauritius (Murday, 2023). Despite this, historical instances of surveillance can be traced back to the French and the British colonial periods, particularly in how they controlled first the slaves, who were treated as mere property, and later the indentured labourers, who were required to carry passes that tracked their movements, while

[1] https://macoss.mu/publications/annual-report/ accessed 24 March 2024.

plantation overseers and managers closely monitored their activities. This system of surveillance was harsh and often accompanied by physical punishment and exploitation. The practices in Mauritius mirror broader imperial strategies of control and exploitation prevalent in other colonial settings (Cormack and Kukutai, 2022). In colonial Africa, state surveillance was a pervasive and frequently brutal feature of colonial rule. Various methods were put in place by European powers to monitor and control local populations for social, political and economic purposes (see Shafer, 2013). At independence, many African governments inherited some aspects of this surveillance state, mainly through the retaining of repressive laws and a partly reformed police and military force, which often continued to function in ways that infringed upon the rights and freedoms of the population (see Akech, 2009; Schmidt, 2013).

Although Mauritius experienced a different form of colonialism and at independence the country quickly instituted coalition and multi-party politics with the goal of providing representation to nearly all ethnic groups, largely due to the Best Loser System (BLS), which is entrenched in the Constitution of Mauritius. The BLS makes provisions for additional seats for MPs from ethnic groups which may be under-represented in Parliament by the first-past-the-post electoral system after each general election. And, with governments based on consent, political rulers have eschewed a standing army. Since there is no army in Mauritius, all military and security operations are handled by the National Police Force (MPF), the Special Mobile Force (SMF) and the National Coast Guard (NCG). The primary purpose of the SMF is to ensure internal security (Murday, 2023, p. 432). The National Mauritian Security Service (MSS) is responsible for the national security of the country.[2] It operates under the Ministry of Defence and has a mandate to gather and analyse intelligence related to national security threats, both domestically and internationally. Managing ethnic relations is one of the most important aspects of domestic security. As a result, the NSS has a desk designated for each of the major ethnic and religious

[2] It was formerly known as the National Intelligence Unit (NIU) and State Security Service (SSS).

communities in the nation: the Chinese, Creole, Hindu and Muslim desks. In certain cases, the NSS has frequently been used for political purposes by succeeding governments and this involves spying on members of opposition parties (Murday, 2023, p. 434).

The absence of conflicts and the maintenance of a relatively stable democracy in Mauritius has averted the use of the panoptical model of surveillance, a growing concern in some African countries. However, the tide is turning and there are fears that the country is moving towards a surveillance state, owing to the democratic backsliding. The move to surveillance started with the 2013 smart biometric ID card, followed by the introduction of the Safe City project in 2017, leading to the mounting of four thousand cameras across the island (Kasenally, 2022a). The government launched the Mauritian Safe City Project (MSCP) to enhance public safety by installing cameras across the island. The project involved three main players, each with distinct yet somewhat unclear responsibilities: the Mauritius Police Force (MPF), the national telecommunications operator Mauritius Telecom, and the commercial supplier Huawei. The overlap between these players, particularly around data management and accountability was a point of contention, as there was limited clarity on how roles were divided and regulated. This ambiguity also raised privacy concerns and calls for clearer oversight mechanisms (Kasenally, 2022a). Critics see the connection between the biometric ID system and the Safe City project because the success of any Safe City project depends on data. The link comes in the issue of data integration. Biometric ID systems collect vast amounts of personal data, such as fingerprints, facial recognition, and other biometric details. In a Safe City project, which often involves widespread surveillance through cameras, monitoring devices and smart city technologies, this data becomes crucial for identification and tracking. With biometric data readily available from national ID systems, authorities can link real-time surveillance footage to individuals, making it easier to track movements, identify suspects and monitor citizens.

Kasenally (2022a, p. 6) argues that, although Mauritius has one of the best data-protection laws in Africa, as well as a Data Protection Office, section 44 of the DPA (2017) stipulates: ‘Personal data shall be exempt from any provision of this Act where the non-application of such provision would, in the opinion of the Prime Minister, be required for the purpose of safeguarding national security, defense or public security.' This clause allows the Prime Minister to reverse the Act's guarantees for the privacy of personal data. According to the Code of Practice for the Operation of the Safe City System(s), this clause applies to Safe City data. There is a potential for abuse, misuse and manipulation of this data, as the terms 'national security' and 'public security' remain undefined in the Act and can be interpreted in broad, flexible ways. When the Safe City and the smart ID card are combined, these concerns are amplified.

In all these developments of the state's attempt to establish a surveillance system, Mauritian society has protested in different forms, leading to the review of the biometric ID, the scaling-down of the Safe City project and the shelving of some problematic proposals to amend the ICT Act requiring that all social-media traffic in the country be decrypted – a move that critics in civil society and the media say amounts to implementing a digital surveillance system (Chan-Meetoo 2021; Phokeer, 2021). Unprecedented in Africa, the public protests over the biometric ID card provide an excellent case study of public oversight.

The biometric ID card: Context and concerns

The National Identity Card Act, which went into effect in 1985, mandated that all Mauritian citizens apply for identity cards no later than six months after turning 18. This card was laminated and had no digital elements.[3] A new system for biometric identity cards was implemented under the Mauritius National Identity Scheme (MNIS) by the Finance (Miscellaneous Provisions) Act 2009 and the National Identity Card (Miscellaneous Provisions) Act 2013, which incorporated on a chip the citizen's biometric information relating to

[3] Human rights and the biometric identity card- Retrieved at https://www.dentons.com/en/insights/articles/2021/july/26/human-rights-and-the-biometric-identity-card, accessed 12 February 2024

external characteristics, such as high-resolution face images, which could enable facial recognition (Baichoo et al., 2018). Furthermore, the 2013 NIC Act's Section 3 mandated the Registrar of Civil Status to maintain a centralised database that stored personal information, biometric data, residential address, national identification number and date of birth maintained in the database located at the Government Online Centre.[4] This is how the government justified the need for a biometric ID:

> Although the National Identity Card (NIC) has served its purpose, it is now outdated and has many flaws. The actual NIC card is paper-based laminated in plastic. This is a major flaw, as it can be easily tampered with. It also lacks security features, which is a major setback, both for national security purposes and for citizen identity management . . . With the fast development in Information and Communication Technology, where security identifications and business transactions are done online, it has become of utmost importance to replace the National Identity Card by a smart version. Amendments to the National Identity Card Act to allow for fingerprints and other biometric information to be incorporated . . . [5]

While smart ID card systems can offer benefits like improved service delivery and convenience, they also carry significant surveillance risks, particularly when they involve the collection and centralisation of personal data. This massive data collection provides authorities with a comprehensive database that could be used for surveillance. Without sufficient legal and regulatory oversight and technical

[4] Section 5 of the NIC Act of 2013 provides that the identity card shall bear the person's names, date of birth, gender, photograph, signature or thumbprint, NIC number and also the date of issue and (in section 5(2)(h)) 'such other information as may be prescribed'. *Madhewoo (Appellant) v The State of Mauritius and another (Respondents)* (Mauritius) From the Supreme Court of Mauritius.

[5] The Prime Minister addressing Parliament: Fifth National Assembly Parliamentary debates (Hansard) Second session Tuesday, 09 July 2013

safeguards, the data collected by smart ID systems could be abused by governments, corporations or hackers. There is also the risk of function creep, where a system initially designed for national identification or public services becomes a tool for broader surveillance activities. Based on these concerns posed by biometric ID card technologies, as stated above, the ID card was resisted by civil society organisations, tech experts and some political actors through an array of mobilisation strategies, including strategic litigation (see Duncan, 2018; 2022).

Theoretical lens

The chapter applies and adapts Kingdon's Multiple Streams Framework (MSF) and political process theory to examine the factors that contributed to successful public oversight of the biometric ID card project. Kingdon (2003) proposes an approach in which three streams – problem, policy and political – are assumed to develop independently from each other with their own agents and dynamics. For an agenda change to occur, all three streams need to be ready for coupling (Herweg at al., 2022). Thus, at certain critical moments, a 'window of opportunity' opens, and the streams come together making policy change more likely to happen. The MSF is used in conjunction with the political process theory, which is a conceptual framework used to understand the dynamics of social movements and their achievement of success. This theory describes the larger socio-political context in which political and social actors operate. It encompasses all the various factors and conditions that influence the opportunities and limitations for political activity and mobilisation. The MSF and political process theory are used as a heuristic tool to generate empirical evidence. From a methodological standpoint, the interpretive methodology employed in the chapter will enable the interpretation and classification of empirical data according to the MSF and political process theory overall structures.

Kingdon's Multiple Streams Framework

Kingdon's MSF refers to a framework used to explain how policy agendas are set and how policies emerge and gain momentum in political systems. The framework which emerged in the mid-1980s, today forms one of the analytical frameworks for understanding public policy agenda-setting. Kingdon writes that, among other things, his framework aims to '[...] try to understand why important people pay attention to one subject rather than another, how their agendas change from one time to another, and how they narrow their choices from a large set of alternatives to a very few' (1995, p. 2).

The MSF approach is universal to most policy processes and provides the flexibility to analyse different contexts (such as countries in the global south) and different policy domains (such as surveillance policies).

The three streams

The *problem stream* consists of issues, challenges or crises that policymakers and the public perceive as requiring attention. Policymakers may pay attention to a very small percentage of issues. Gaining attention is a significant accomplishment that must be addressed right away to prevent focus from going elsewhere (Birkland, 1997). *The policy stream* encompasses various solutions, proposals or policy ideas that have been developed by experts, interest groups or government agencies to address specific problems. These advocates of policy proposals may be considered 'policy entrepreneurs' or agents for policy change (CSOs, political elites). According to Kingdon, policy solutions are like a 'policy primeval soup', changing over time as one actor proposes them, then others reconsider and modify them. According to Kingdon (1995, p. 140), 'accumulation of knowledge amongst the policy community contributes to the generation of ideas'. *The political stream* consists of four core elements: organised political forces, change in government, the political climate, including the mood of the public, and the bargaining process. These elements can create windows of opportunity for certain policies to be adopted. The policy window, according to Kingdon, is the opportunity to take certain proposals forward (Kingdon, 1995, p. 166). Policy windows emerge through alignment among specific policy problems, political forces and proposed policy responses. During policy windows, it becomes possible for change to occur, driven by the agenda setting of policy entrepreneurs (Kingdon, 1995, p. 168).

Although it is acknowledged that the Kingdon framework would not be able to identify every macro- and micro-force and factor at work, the framework can nevertheless provide important insights into Mauritius's policymaking process for smart ID cards and make a valuable contribution to the body of knowledge on public oversight. Public oversight for the purposes of this chapter refers to the mechanisms and processes through which citizens, civil society organisations and institutions monitor and influence the actions and decisions of public bodies and propose policy solutions. Hence, the goal of this chapter is to examine its portability and provide a road map for researchers wanting to apply the framework to understand how public oversight happens in each context.

Political process theory

Political process theory emphasises the importance of political opportunities, mobilising structures, and framing processes in shaping the trajectory and outcomes of social movements (Tarrow, 1996; Fillieule and Accornero, 2016). This chapter focuses on the first two factors – political opportunities and mobilising structures. Although framing processes, which involve how movements present their issues and craft narratives that resonate with the public to gain support, are important, this research does not delve into that aspect. It does not specifically examine the narratives that influenced the smart ID protests.

Political opportunities refer to elements of the political environment that affect a group's capacity to mobilise effectively (Koopmans, 2004, cited in Giugni, 2009, p. 361). Scholarship has identified four key aspects of political opportunities: (1) the degree of openness or closure of the institutionalised political system, (2) the level of stability or instability within that system, (3) the presence or absence of elite allies, and (4) the state's capacity and inclination for repression (McAdam, 1996, p. 27). These four dimensions structure the discussion in this chapter. Mobilising structures include the groups, organisations and formal or informal networks that facilitate the mobilisation of individuals and resources. Effective mobilising structures often involve social networks, community groups and pre-existing institutions that can be leveraged to strengthen the movement (Tarrow, 2011).

Framing biometric ID system as a problem

The biometric ID card was introduced under the Labour Party/ Mauritian Social Democratic Party (PMSD) coalition government led by Prime Minister Navinchandra Ramgoolam, who was serving his consecutive second term (2004–14), or third non-consecutive one. The government, as mentioned above, stated that the biometric system was part of broader efforts to enhance national security, streamline public services and create a robust national identification system. However, citizens, pressure groups and civil society organisations (CSO) and trade unions rallied with the socialist political organisation Lalit du Klas (henceforth Lalit), an extra-parliamentary party, raised concerns regarding privacy and data protection, particularly in relation to how biometric data would be stored and used by the government.

Lalit cited the negative experiences with biometric ID cards in the UK, Australia and the USA, where both lawmakers and the public rejected these cards and their centralised databases. Lalit said:

> Having to produce a card for the Authorities is hurling us back to the times of slavery and indenture. It is hardly modern to do this. The people of three quite 'modern' countries, Australia, the USA and Britain, have risen up against their governments and managed to stop biometric ID cards, even when they had

> begun to be introduced, as they are here now. They signed petitions, held meetings, put up YouTube messages, organised debates and they were very slow to go and take up the cards. Eventually, so many people in these three countries opposed the biometric data centralisation, that the respective governments had to back-pedal and get the cards and database destroyed.[6]

It also conducted research on the failure of biometric ID cards in other countries where there were serious data leaks – Israel, India and South Korea.

This international research and coordination done by Lalit members has shown us all how people worldwide have opposed and are still successfully opposing this kind of surveillance, and it has also shown how the imperialist countries have taken a lead in trying to get these types of card-system into place worldwide for surveillance. But the fact that the masses of the people, often led by left parties, have seen the dangers and possible abuses in time, has meant that the cards are being challenged everywhere.[7]

Pressure groups, in the form of Lalita and Rezistans ek Alternativ[8] and technical experts not only underlined the threats of the centralised biometric ID to human rights and privacy, but also questioned the business interests behind the smart ID. Lalit conducted

[6] Lalit (2013) Lalit addresses students on dangers of the new ID cards. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1537/lalit-addresses-students-on-dangers-of-the-new-id-cards/, accessed on 23 March 2024.

[7] Lalit (2014) Elections IX: Freedom Infringed: Danger of the New ID Card. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1669/elections-ix-freedom-infringed-danger-of-the-new-id-cards/, accessed on 23 March 2024.

[8] Rezistans ek Alternativ is a political movement and party in Mauritius that is known for its focus on social justice, human rights, environmental sustainability and equality. The movement is seen as a voice for the marginalised, and it operates outside the traditional political framework, challenging the established political parties on issues such as governance, fairness and social equity.

research on the financial ramifications behind the project.[9] The government signed an agreement with the Singapore Cooperation Enterprise on 17 October 2012 for the implementation of the card to the tune of Rs1.152 billion Mauritian rupees (equivalent to around 28.8 million USDs).[10]

It is important to note that at this time, the idea of a biometric ID card and its implications were not well known among ordinary people in Africa,[11] and this was not different in Mauritius. As a result, the public did not have enough information: 'The public was suspicious of the government's intentions but did not know enough about the system to oppose it . . . according to Mauritian information specialist and open-source advocate Ish Sookun, the system was a "black box for them, they didn't know what was inside"' (Duncan 2022, p. 171).

CSOs and human-rights and technical experts framed the issues in ways that people could understand. Lalit provided evidence-based insights that were accessible and understandable to the public. Rezistans ek Alternativ also raised concerns of the biometric ID card, especially in relation to the privacy of data. The organisation raised the issue that, although the card only contained minutiae, or biometric data in electronic format, the law could be amended at any time according to section 10 of the NIC Act, and other data (for example, medical or banking) could thus be included on the card because this article of the law did not impose any limits.[12] Here the concern was the potential secondary use of data that would extend far beyond its original purpose and without explicit consent.

[9] Lalit (2014) Brief summary of Lalit actions against compulsory biometric ID card system. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1763/brief-summary-of-lalit-actions-against-compulsory-biometric-id-card-system/ accessed 23 March 2024.

[10] Hansard, 29 September 2015.

[11] Although scholars in Africa were already debating the issue of digital IDs (for example, Keith Breckenridge (2014) 'Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the present').

[12] Biometric identity card: the fear of protesters, L'Express. Retrieved at https://lexpress.mu/article/309881/carte-didentite-biometrique-frayeur-contestataires, accessed 24 May 2024.

Stéphan Gua, member of Rezistans ek Alternativ pointed to the danger of the scheme:

> The law states that the biometric identity card can store data without defining it. However, the responsible minister or the Prime Minister plans to amend the law to include other biometric data . . . the danger lies in the fact that an individual will not know what data the company (banks, medical institutions) can have access to.[13]

The No to Biometric Data on ID Card platform raised the concern of identity theft. Activist Jeff Lingaya from this platform stated:

> This would mean that companies designated by the State will be able to collect the fingerprints of any individual who visits the company in question. In addition, thanks to this data, they will be able to have all the information about this person . . . in extreme cases, this can give rise to identity theft.[14]

These advocates for policy proposals, also called 'policy entrepreneurs' (Leon-Espinoza 2022), became instrumental in advocating for their preferred policy solutions. MSF argues that conditions must be turned into public problems to become relevant for the policy process. In democracies, a wide range of actors can serve as problem brokers, leveraging the media to bring public attention to various issues. These actors include advocacy or interest groups, academia, political actors and journalists (Herweg et al., 2022). Pressure groups (such as Lalit) and technical experts proposed alternatives to the centralised biometric ID system. In an interview with the media where he works, Ish Sookun, a technical expert and open-source advocate, outlined some of the proposed alternatives. They suggested a distributed identity management system that facilitates automated information updates across several government departments (Duncan, 2022, p. 173).

[13] Ibid.

[14] Ibid.

At the core of the pressure groups was the rejection of the biometric ID card in its original form, based on grounds of social justice. Some of the key justice issues include the right to free movement, as articulated by Lalit in one of their campaign materials:

> Until now, it is not compulsory to present an ID card to anyone. As from next year in October, 2014, according to the National ID Card Act 2013, you will have to present your card to anyone who, by law, can call on you to do so, or to 'every' one else with reasonable authority. If you do not produce it on-the-spot, the person can 'direct' you as to who to present it to, within what delay, and where. This means back to the times of indenture when you needed papers in order to leave the Sugar Estate you were assigned to. There goes our freedom of movement, won less than one hundred years ago.

Lalit further argued that the ID card may be required for accessing public services, transportation or even entering certain areas. If individuals cannot or do not wish to provide their biometric information, they may be restricted from moving freely, impacting their right to freedom of movement. As Couldry and Yu (2018) argue, in the age of big data and datafication, the monitoring of individuals and groups through digital surveillance can exacerbate power imbalances and cause further harm.

Mobilisation structures

McAdam (1982) initially characterises mobilising structures as the organisational resources accessible to a discontented populace, facilitating their ability to capitalise on opportunities within the political arena and organise effectively. Subsequent definitions from McAdam et al. (1996), go from the concept of 'resources', implying a passive function, to the more dynamic notion of 'collective action' (cited in Hauwaert, 2021, p. 89). Collective action refers to strategies. Thus, mobilisation strategies within political process theory refer to the methods and tactics used by interest groups or social movements to influence policy decisions, public opinion and the broader political system. These strategies are crucial in shaping policy outcomes by gathering support, raising awareness, and exerting pressure on decision makers. Mauritius mainly used three strategies – protests/campaigns, political lobbying and strategic litigation. The media in Mauritius also played a key role in disseminating information and raising awareness about the potential risks associated with biometric ID cards. The newspaper *L'Express*[15] ran several articles on the different sides of the debate on the issue. Activists also used radio to raise awareness. Radio is deeply intertwined with everyday life in Mauritius, as in many African countries (see Gunner et al., 2012) and is, therefore, highly popular among the public (Chenganna, 2022).

Protests and campaigns

Lalit organised workshops, protests and campaigns to raise awareness and challenge the biometric ID system. The campaigns drew in opposition political parties and were supported by a broad coalition of individuals, including former presidents, a former attorney general and other prominent figures in Mauritian society. Duncan (2023) writes that initially disparate campaigns against smart ID, which sprang organically, remained separate. But as the campaign organised by Lalit caught the attention of opposition political parties and some governments officials, the opposition coalesced into a somewhat unified campaign. Lalit explains it this way:

> The political campaign initiated by Lalit and other trade union and social organisations . . . gradually galvanized wide support and gathered enormous political momentum. Eventually, even the Parliamentary Opposition led by Bérenger and Jugnauth

[15] *L'Express* is a French-language daily newspaper, published in Mauritius since 1963 and owned by La Sentinelle, Ltd. It endeavours to cover Mauritian news in an independent and impartial manner. It is the most widely-read daily in Mauritius.

> changed its stand; having approved the new biometric cards in Parliament, they actually took a stand and opposed them.

In 2013, when the Labour Party had introduced the Mauritius National Identity Scheme (MNIS) Project, the opposition had supported the biometric ID card as evidenced in the statement below:

> We, on this side of the House, had the possibility in the past, Mr Speaker, Sir, of expressing our disagreement with the way this project was introduced. The House will remember how my predecessor, the Leader of the Opposition then, hon. Paul Bérenger, in fact, in this very House expressed, again, the objection and the way in which the whole project had been introduced, had been ushered in with the Singapore authorities. We have not changed our minds since that, Mr Speaker, Sir. We are still on the same wavelength of not agreeing to the way this MNIS project has been introduced. Be that as it may, Mr Speaker, Sir, as far as the proposal in this Bill, we don't have any quarrel . . . We have no quarrel with these proposals and amendments.[16]

From this statement, it is clear that the only disagreement the opposition had with the ID card was the procurement process for the service provider but they supported the idea of the biometric ID in its form.

Public opposition to the new ID cards also gained momentum after it was revealed that a hard disk containing biometric data had gone missing from a government building. This incident, along with computer expert Ish Sookun's exposure of security vulnerabilities in the way the data was being stored, fuelled further concerns including among the opposition politicians.[17] The campaigns attacked not only the central database, but also the 'oppressive system that

[16] Hansard, 29 September 2015.

[17] Iqbal Ahmed Khan (2021) From biometric ID cards to Safe City cameras, how our civil liberties are impacted. *L'Express*. Retrieved at https://lexpress.mu/s/article/387343/biometric-id-cards-safe-city-cameras-how-our-civil-liberties-are-impacted, accessed 27 March 2024.

underpinned it and argued that opposition needed to be part of a broader political struggle for more freedom, less surveillance and less oppression' (Lalit 2017, cited in Duncan 2022, p. 172). However, Lalit was against the idea of the card in its totality. This organisation had shown resistance to the ID card since the first plastic card was introduced in 1986.

> In 1986, Lalit opposed the first ID Cards, when they went through the Cabinet, and were in fact introduced. We considered even those ordinary cards to be the thin end of a wedge of surveillance and infringement on freedom of the people. We objected to the cards as being a kind of 'pass'. We believed that they would increasingly be demanded prior to people getting ordinary access to their rights. We were not wrong. Since then, Lalit has continued to take position every time we were threatened with the new 'Smart Cards', starting in 1996. Even then, we opposed the centralized storage of data on citizens, whether in relation to elections, health or any other data.[18]

Lalit collaborated with approximately 18 other organisations to protest against the new card, highlighting its various dangers, such as risks to privacy, data security and the potential misuse of personal information and the potential for surveillance. Together, they organised a petition endorsed by these organisations. Lalit spearheaded a nationwide campaign that included distributing bulletins at workplaces and universities using a mobile van, as well as hand-delivering leaflets and letters to Village Councillors across the country. In Mauritius, Village Councils are local governance bodies responsible for the administration and management of rural areas. They play a crucial role in ensuring the efficient delivery of public services, promoting local development and addressing community needs.[19] In

[18] Lalit (2014) Elections IX: Freedom Infringed: Danger of the New ID Card. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1669/elections-ix-freedom-infringed-danger-of-the-new-id-cards/,accessed on 23 March 2024.

[19] The Local Government System in Mauritius: Country Profile 2017–18. Retrieved

December 2013, Lalit organised a 'go-slow', which was widely followed by the public. In another unique protest strategy, in March 2014 Lalit served a citizen's 'Notice' on all staff at the Mauritius National Identity Scheme offices. 'This decentralized action warned staff not to act illegally and against the Constitution by putting pressure on members of the public to give biometric data for storage.'[20] The campaign also involved door-to-door visits in selected areas where Lalit explained in detail, household by household, what the dangers of the biometric ID were.

The protest movement reached its peak with a demonstration at the Registrar General's Building, which housed the primary ID Card Conversion Centre in July 2014. The purpose of the protest was to submit individual protest letters after being denied registration for an ID card due to their refusal to provide fingerprints.[21] This followed dozens of people who went to the National Identity Card Centre to request an ID Card without consenting to be fingerprinted or to have any biometric photograph taken. The officials at the Card Centre present refused to process the applications.

According to MSF, policy entrepreneurs' selection of strategies importantly relates to the context and suggests four processes in the political stream discussed earlier. Organised political forces including political parties, interest groups and coalitions influence policymaking; changes in government to refer to shifts in leadership or political control can open or close windows of opportunity for policy change; the national mood or public opinion plays a critical role in shaping the political context and the bargaining process refers to the negotiation between different stakeholders involved in policymaking. These processes can create windows of opportunity for certain policies to be adopted (Leon-Espinoza, 2022). Regarding

at https://www.clgf.org.uk/default/assets/File/Country_profiles/Mauritius.pdf, accessed 4 February 2024.

[20] Lalit (2015). Brief summary of Lalit actions against compulsory Biometric ID card system. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1763/brief-summary-of-lalit-actions-against-compulsory-biometric-id-card-system/, accessed 23 March 2024.

[21] Ibid.

the first process, organised political forces, or policy entrepreneurs in Mauritius exhibited a high degree of consensus that positively led to successful public oversight. Change in government also played a role in the amendment of the biometric ID card. The MSM political party, under Anerood Jugnauth, came into power in December 2014, a year and a few months after the biometric ID card was introduced and this provided an opportunity for policy change and effective public oversight. The smart ID card had become one of the rallying points in the 2014 elections. The national mood between 2013– and 2015 was one of opposition to the smart ID system. Opposition leaders in Parliament and social movements/CSOs kept the issue on the agenda through various activities discussed above. During this period, the bargaining processes involved policy entrepreneurs who became instrumental in pushing for the amendment of the biometric ID card with the support of political agents.

Political lobbying

Mauritius has a vibrant political culture. As discussed earlier, the opposition is a crucial component of Mauritius's political system, with the position of opposition leader specifically outlined in the country's Constitution. The opposition, headed by an MP nominated by the President, based on the leading minority party in the house presidential appointee, plays a vital role in holding the government accountable in parliament (Bertelsmann Stiftung 2024, p. 9). The coalition-building approach in the country helps in fostering consensus among diverse political parties and communities. As a result, the process promotes inclusivity by ensuring that various groups are represented in governance, while also encouraging moderate policy-making that caters to a broad spectrum of interests (Srebrnik, 2000; Sithanen, 2003; Mehta, 2015). Government positions, including cabinet posts, are generally distributed to maintain ethnic balance. When the biometric card was introduced in 2013, the opposition party was led by a coalition called the Lepep Alliance that included the Militant Socialist Movement (MSM) led by Aneerood Jugnauth, the Mauritian Social Democrat Party (PMSD) of Xavier Luc Duval and the Muvman Liberater (ML) led by Ivan Collendavelloo. Kasenally and Ramtohul (2020, p. 4) states that 'systematic pre-electoral coalitions are an important feature that has defined postindependence politics'. The alliance, in which Pravid Jugnauth acted as the prominent figure on the issue, opposed the biometric ID card, spurred by lobbying efforts from civic groups led by Lalit:

> Instead of the MMM and MSM denouncing the whole procedure in Parliament, they just went along with it, with Alan Gannoo when he was Leader of the Opposition even saying they had 'no quarrel' with it. When protests nation-wide began to build up, then they changed their stand . . . he MSM and MMM thus 'tail-ended' the mass movement set in movement by LALIT.[22]

These groups successfully influenced both the opposition alliance and the Leader of the Opposition in Parliament through a sustained campaign that involved a strategic focus on rights, privacy and potential misuse of biometric data, which possibly helped to galvanise political alliance. The subsequent opposition leader, Paul Berenger of the Mauritian Militant Movement (MMM) party challenged the smart ID and demanded the destruction of the central database. The ID card issue became a central theme in the December 2014 elections. The Lepep coalition, headed by Anerood Jugnauth, achieved a landslide victory. Once the Lepep coalition got power, the civic groups promptly submitted a petition signed by eight organisations, urging the new government to continue their action against the biometric ID.[23] In February 2015, Lalit sent a letter to all

[22] Lalit (2014) ELECTIONS IX: Freedom Infringed: Danger of the New ID Cards. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1669/elections-ix-freedom-infringed-danger-of-the-new-id-cards/ accessed 20 June 2024.

[23] The petition was signed by organisations: Confederation of Independent Trade unions, Muvman Liberasyon Fam, Centre Idriss Goomany, Confederation Travailleurs Secteur Prive, Labaz intersindikal, Playgroups, ACIM, LALIT ('Petition to the new government on ID Card measures'. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1694/petition-to-the-new-government-on-id-card-measures/ accessed 20 June 2024.)

MPs and ministers in the newly elected Lepep Alliance, reminding them to fulfil their promise to oppose the biometric ID cards.[24] The alliance government announced formally in its President's Speech that it would destroy the database:[25] 'The data bank containing fingerprints and biometric photographs of the new National Identity Cards will be destroyed to protect sensitive personal data of our citizens.'[26]

The Prime Minister was also petitioned by Lalit and 11 other organisations in July 2015 following the Supreme Court Judgement and Injunction discussed below to destroy the database.

Strategic litigation

In response to the public uproar and resistance to the new smart ID from civil society organisations and opposition parties, Maharajah Madhewoo, an activist and then-opposition leader Pravind Kumar Jugnauth, filed two constitutional challenges with the Supreme Court in 2015. In the first, the validity of the government's fingerprint collection process for ID cards was questioned, and in the second, the storing of fingerprints in a central government database was called into doubt. Madhewoo chose not to apply for the biometric card and argued that the legislation governing the collection, retention and storage of his biometric data constituted an unjustified violation of his fundamental rights as protected by the Constitution. He challenged the constitutionality of the 2013 Act by seeking

[24] Lalit (2014) 'Petition to the new government on ID Card measures'. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1694/petition-to-the-new-government-on-id-card-measures/ accessed 20 June 2024.

[25] Lalit (2015) Victory approaching for destruction of ID Card database. Retrieved at https://www.lalitmauritius.org/en/newsarticle/1742/victory-approaching-for-destruction-of-id-card-data-base/ accessed 20 June 2024.

[26] Government programme 2015–19: Achieving Meaningful Change – Address by the President of the Republic of Mauritius, Tuesday, 27 January 2015, p. 57. Retrieved at https://mauritiusassembly.govmu.org/mauritiusassembly/wp-content/uploads/2023/03/govprog2015.pdf.

redress under section 17 of the Constitution. This section enables individuals to apply to the Supreme Court for relief if they claim that any provisions from Sections 3 to 16 of the Constitution, which outline fundamental rights and freedoms, 'have been, are being, or are likely to be violated in relation to them'.[27] The Supreme Court ruled that while it was not unlawful for the government to collect fingerprints for the purpose of issuing new ID cards, it found that storing and retaining biometric fingerprint data in a single database was unconstitutional. The court found that:

> . . . the law providing for the storage and retention of fingerprints and other personal biometric data regarding the identity of a person constitutes a permissible derogation, in the interests of public order, under section 9 (2) of the Constitution . . . the provisions in the National Identity Card Act and the Data Protection Act for the storage and retention of fingerprints and other personal biometric data collected for the purpose of the biometric identity card of a citizen of Mauritius are unconstitutional.[28]

Madhewoo also challenged the validity of the smart ID card before the Judicial Committee of the Privy Council, particularly over the violation of an individual's fundamental right to privacy. In the case of *Jugnauth v Mauritius*, the claimant challenged the National Identity Card (Particulars in Register) Regulations 2013, which permitted the storage and retention of 'fingerprints' and 'encoded minutiae of fingerprints' in a register created under sections 3(2)(b) and 10 of the NIC Act 2013. Jugnauth argued that these provisions violated sections 3(a), 3(c), and 9 of the Constitution. As part of the case, he sought an injunction to prevent the defendants from storing his fingerprints and biometric data in the database (Baichoo

[27] The Constitution of the Republic of Mauritius. Retrieved at https://cdn.accf-francophonie.org/2019/03/maurice-constitution2016.pdf.

[28] *Madhewoo M. v The State of Mauritius and ANOR* (2015 SCJ 177). Retrieved at https://ionnews.mu/wp-content/uploads/2015/05/Biometric-ID-Card_Madhewoo-vs-State.pdf, accessed 8 March 2024.

et al., 2018, p. 5). The court held that the storage of the data was not sufficiently secure because the safeguards of the Data Protection Act were not sufficient, and the storage of the data was not subject to judicial scrutiny and control.[29] A similar verdict was delivered in Jugnauth's personal case before the Supreme Court. The Privy Council affirmed the Supreme Court's findings in October 2016 (Baichoo et al., 2018).

The government published the National Identity Card (Civil Identity Register) Regulations 2015 in response to the Supreme Court's decision. These regulations restricted the storage of relevant data to the identity card itself, as opposed to a central register. This type of regulation is implemented to protect privacy, reduce the risk of large-scale data breaches and limit government or institutional surveillance. It ensures that personal information remains secure and under the individual's control, rather than in a potentially vulnerable centralised repository. Based on cabinet papers, the government assigned the Singapore Corporation Enterprise the responsibility of eliminating all fingerprint images and minutiae from the Mauritius National Identity Central Database, including all backup tapes.[30] Therefore, fingerprint details are now only collected to issue identity cards; thereafter, they are erased and are only stored as minutiae on the cards that the people own.

Later, through the Finance Act of 2017, the government revised the NIC Act to encourage the adoption of Secure Access Module (SAM) card readers for card verification, which eliminates the need to duplicate and store card data. This implies that the card may only be used for identification when the citizen is physically present, and their fingerprint is matched to the detailed information contained on the card. The new procedure would therefore differ from the prior one, as it no longer needed a central database. Furthermore, the Data Protection Act of 2004 was abolished and replaced with

[29] *Madhewoo (Appellant) v The State of Mauritius and another (Respondents)* (Privy Council Appeal No 0006 of 2016). Retrieved at https://www.jcpc.uk/cases/docs/jcpc-2016-0006-judgment.pdf, accessed 8 March 2024.

[30] Fingerprint minutiae are defined in the legislation as 'the characteristics of a fingerprint image such as the ridge endings and ridge bifurcations'.

the Data Protection Act of 2017 to improve data subjects' control and personal sovereignty over their personal information. In Mauritius, the right to privacy is constitutionally protected, and citizens are entitled to anticipate that this right would be respected and maintained. Nevertheless, because the 2014 Data Protection Act was passed prior to the development of biometric technology in the nation, it was not appropriate for the storage and security of biometric data. The Data Protection Act 2017 addresses this main shortcoming by providing organisational and technical measures 'to prevent unauthorized access to, alteration, disclosure, accidental loss and destruction of personal data . . . including confidentiality, integrity, availability, and resilience of processing systems' (Baichoo, 2018, p. 7). Special categories of personal data now explicitly include genetic data or biometric data in line with subjects over their personal data, and to comply with international data protection norms regarding automatic processing of personal data.

Madhewoo, who had lodged a legal challenge against the ID card system in the Supreme Court, subsequently approached the UN Human Rights Committee in December 2017 to challenge the collection and retention of biometric information on ID cards. He said that this practice infringed upon his right to privacy. He argued that, if the smart identity card was lost or stolen, fingerprint data might be copied onto counterfeit cards, and that giving citizens the responsibility for storing the biometric data was a security vulnerability. The United Nations Human Rights Committee (HRC) ruled on 24 March 2021 that the existing identity-card program breaches individuals' private rights, as outlined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). The Committee urged the Mauritian government to reassess the reasons for keeping fingerprint data on identity cards considering the existing data security concerns, and to offer Madhewoo a viable resolution.[31]

[31] United Nations Human Rights Office of the High Commissioner (2021) *Mauritius: Storing biometric data on identity cards violates privacy – UN Human Rights Committee*, retrieved at https://www.ohchr.org/en/press-releases/2021/07/mauritius-storing-biometric-data-identity-cards-violates-privacy-un-human?LangID=E&NewsID=27329, accessed 5 December 2023.

Factors explaining successful mobilisation and prospects for the future

Analysing the factors that led to the successful mobilisation against the biometric ID card is essential to understanding whether the success stemmed from unique circumstances specific to that historical period (2013–15) or if it was influenced by inherent characteristics of Mauritian society. The successful mobilisation can likely be attributed to a combination of specific historical circumstances and deeper societal factors. First, it is important to remember that around the time of the proposed implementation of the biometric ID card in 2013, global concerns about privacy and data security were rising. Snowden revelations were released that same year and highlighted the potential misuse of personal data, and this could have fuelled local resistance. Second, the decision to implement biometric ID cards was made by the government at a specific time when there was heightened political sensitivity and scepticism towards government policies in the country. Although Mauritius has a stable democracy, the ruling party under Labour/MMM coalition were accused of corruption and economic mismanagement (Ramtohul and Hylland, 2018). Third, the political climate significantly contributed to the opposition against the biometric ID card, introduced a year before a crucial election in Mauritius. Two main alliances contested the election: the Lepep Alliance (comprising the MSM, ML and PMSD) and the Labour/MMM Alliance (a coalition between the Labour Party and MMM). The election resulted in a significant political shift, with Alliance Lepep winning a landslide victory, securing 47 out of 62 directly elected seats. Anerood Jugnauth returned as Prime Minister after two years in political retirement. This election was also viewed as a referendum on proposed constitutional reforms, which sought to increase presidential powers, especially as the proposal would place the outgoing Prime Minister as the first President with such powers.[32] Voters rejected these

[32] The political system is based on the Westminster style of government where the Head of State (being the President) is a ceremonial figurehead with very few executive powers.

reforms, and the opposition's campaign resonated widely. The Lepep Alliance, as previously mentioned, capitalised on the protests against the ID card as a key point in their election campaign. The election of Anerood Jugnauth of MSM in December 2014, whose son Pravind Jugnauth had initiated a constitutional case against the smart-ID system, also presented an opportunity. However, these three factors, which undoubtedly opened an opportunity or 'policy' window as Kingdom argues, are not enough to explain the successful mobilisation against the biometric ID card. Other factors, endemic to Mauritius historical and socio-political conditions explain the successful public oversight of the threat to digital surveillance in the country. Cultural values, colonial history, active civil society, robust legal framework and historical legacies embedded within Mauritian society also played a crucial role.

Cultural values and colonial history

Mauritian society has inherent concerns about privacy and the potential for governmental overreach. The idea of biometric data collection and centralised storage by the state was certainly seen as an infringement on personal freedoms. This emerges from Mauritius's colonial history of slavery and indentured labour that instilled a certain wariness of centralised control and documentation. The British took control of the island in 1810 and, following the abolition of slavery in 1835, they brought Indian indentured labourers to work in the sugar-cane plantations, replacing the former slaves (Ramtohul, 2021, p. 831). These labourers were subjected to stringent surveillance and control mechanisms by the colonial authorities to maintain order and productivity on the sugar plantations. Labourers' movements were restricted through pass systems that required them to obtain permission to leave the plantation for any reason. This surveillance is akin to approaches used to control and managing indigenous peoples elsewhere as part of colonisation (Cormack and Kukutai, 2022).

Despite the surveillance, labourers found ways to resist through acts of defiance, slow work, escapes and forming clandestine networks to communicate and support each other. From the early 1900s the local population, mostly constituted of indentured labourers, became politically aware and organised (Kasenally and Ramtohul, 2020). The indenture system produced a significant labour movement which was at the heart of the fight for universal suffrage and for the independence of the country (Allen, 1999; Kasenally and Ramtohul, 2020). Indentured labourers were required to always carry identification cards, resulting in widespread animosity against compulsory identification systems. Given this history, the implementation of the smart-ID-card system brought back memories of this repressive history and fostered a widespread awareness of the potential dangers associated with such systems (Duncan, 2018, p. 64).

Active civic networks

Mauritius has a relatively vibrant civil society with active NGOs and advocacy groups. The Mauritius Council of Social Services has over 390 NGOs registered and estimates that about 8,000 voluntary organisations operate in the country.[33] These trends help explain the unusual vitality of democracy in Mauritius, even though most of these NGOs are funded by the state. NGOs have a significant impact on policy and are consulted by the government during the preparation of the national budget. Their role in combating social inequality and advocating for social justice is acknowledged (Bertelsmann Stiftung, 2024). The diverse ethnic make-up of Mauritian society has not been a hindrance; instead, it has enriched the nation's democratic culture. The pluralistic nature of Mauritian society has fostered a culture of tolerance, dialogue and mutual respect and supports a collaborative approach to addressing the nation's social challenges (Kasenally, 2011). It can be argued that this strong foundation made it relatively easy to mobilise civil society and the public to protest against the introduction of the biometric ID card.

[33] MACOSS Annual Report (2019). Retrieved at https://macoss.mu/wp-content/uploads/2021/01/MACOSS-ANNUAL-REPORT-2019.pdf, accessed 8 March 2024.

Political opportunities

The broader political environment of Mauritius also helps us to understand how collective action and public oversight happens. As McAdam et al. (1996) argue, there is a correlation between institutionalised politics and social movements. Political opportunity theories posit that social movements and revolutions are shaped by the broader set of political constraints and opportunities unique to the national context in which they are embedded. The four dimensions of 'political opportunity structures' (McAdam, 1996) mentioned earlier help explain the success of public oversight. The first one relates to openness or closure of the *institutionalised political system*. As mentioned earlier, Mauritius inherited a vibrant and competitive political culture and can be regarded as relatively open, and politics takes place in a framework of a parliamentary democracy. Legislative matters are closely monitored by citizens, and the law is generally viewed as a protector of civil rights (Ramtohul and Hylland, 2018; Kumar, 2019). The law and the courts have legitimacy, and this augurs well for public oversight, although trust levels have decreased over time. These institutional structures in Mauritius have created a healthy environment for oversight – both state and public. The second dimension about stability of *elite alignments* is the key to understanding the prevailing political culture in Mauritius. The four main parties – the MSM, MMM, Labour Party and PMSD – have governed the country since independence. This institutional political system is more open to traditional forms of civic activism. The two dimensions are related in the sense that in highly institutionalised systems, elites often align with institutions and influence political decisions through formal channels like party membership and lobbying, stabilising competition within established procedures. In less institutionalised systems, where formal institutions are weaker, elite alignments rely more on personal networks, clientelism and patronage, leading to unpredictable and unstable power struggles (Higley and Burton, 2006; Acemoglu and Robinson, 2012). The third dimension relates to the presence of *elite allies*. As discussed above, individual politicians who have a particular interest in advocating for human rights were key elite allies who fought against the smart biometric ID card. These elites were mainly from opposition politicians who used their position to assist the movement. The last dimension is the state's capacity and *propensity for repression*. Mauritius is generally considered to have low levels of state repression, especially in comparison to many other countries in Africa. This perception is supported by various factors, such as democratic governance, rule of law and judicial independence, media freedom and a relatively restrained police force (Ramtohul and Eriksen, 2018; Freedom House, 2024).

In conclusion, while there were policy openings and political opportunities between 2013 and 2015 that made successful public oversight possible, Mauritius is a nation with deeply ingrained democratic institutions and a strong mobilising spirit that makes public oversight a possibility. The protests against possible digital surveillance did not end with the biometric ID card but were reflected a few years later in 2019, when the government introduced the Mauritius Safe City Project (MSCP) funded by Huawei. CSOs and experts questioned the civil liberties aspect of the project. Opposition parties argued that the MSCP could be used to keep tabs on and retaliate against political opponents and their supporters (Kasenally, 2022a). There were reports of citizens decommissioning the CCTVs (Duncan, 2022). In 2021 the state's attempt to extend its digital capabilities through a plan to regulate the use and addressing the abuse and misuse of social media was met with massive local and international pushback (Kasenally, 2022a). The state proposed to amend the Information and Communications Technologies (ICT) Act to mandate the Mauritian regulator to decrypt all web traffic judged to be 'social media' by interfering with issuing security certificates for HTTPS traffic, which would then be routed through proxy servers under the authority of the government (AccessNow et al., 2021). Under international human-rights norms, this proposed regulatory framework had two serious flaws: administrative censorship that would have a chilling effect on freedom of expression and the disablement of encryption, which is essential for digital security (AccessNow et al., 2021; Phoker 2021). Additionally, the proposed legislation violated the data protection laws in the country (Mwesigwa, 2021). Civil society organisations strongly opposed the plans, and sections of the media criticised the strategies employed to advance them. Thus, local CSOs and international digital-rights organisations have expressed concern about the proposal's potential effects on Mauritius's right to privacy and freedom of speech. The ICTA proposal was also 'in fact, aimed at suppressing dissent on social media platforms, which have become extremely popular civic fora for politicians, CSOs and ordinary citizens' (Kasenally, 2022b; p. 13). ICTA received more than 1,500 public responses regarding the proposal. This outcry caught the attention of international digital-rights organisations and subsequently issued a 'joint civil society statement' urging the Mauritian government and ICTA to withdraw the consultation document. Observers attribute the proposal's rejection to a collaborative effort by local and international civil society organisations (Kasenally, 2022b, p. 13).

The biometric ID-card protests created a consciousness around digital surveillance in the country as citizens have now become suspicious of any move towards a surveillance state (Duncan, 2022). However, the prospects for public oversight in Mauritius going forward are uncertain. There is democratic backsliding taking place in the country as stated earlier (Ramtohul, 2018; Kasenally and Ramtohul, 2020; Kasenally, 2022b). Authoritarian measures have reined in civil liberties, including the introduction of a biometric ID card in 2013, arrests of journalists in 2019, multiple suspensions of a commercial radio station's licence in 2020 and the political capture of key institutions including the legislature, where Opposition Members of Parliament have been recurrently expelled between 2020–21 (Kasenally, 2022a). In 2021, the Cybersecurity and Cybercrime Act and the Independent Broadcasting Authority (Amendment) Act were adopted in the Mauritian parliament despite wide public protests. In 2021, thousands of Mauritians took to the streets of the capital, Port Louis, demanding the resignation of the government over allegations of corruption and fraud. The protesters responded to opposition parties' appeals to hold political leaders accountable. They marched to the office of Prime

Minister Pravind Jugnauth.[34] The government is also facing criticism over its transparency and mismanagement of a massive oil spill in August 2020. For the first time in its history, armed militarised police were deployed against peaceful protesters in the capital city in 2021.

The political system in the country is also becoming increasingly leader-centric as it continues to be dominated by a few families. Power and decisions are concentrated, focused on big money and growing levels of cronyism and ethnic divisions are increasingly prominent in politics (Kasenally, 2022a; 2022b). For example, the contract for biometric ID cards given to Singapore Cooperation Enterprise was a government-to-government agreement strictly kept under wraps and done without going through any tendering exercise. The same happened years later with regards to the Safe City project. Despite these negative developments, Mauritius has demonstrated the significance of media, CSOs and citizens as crucial components of the oversight system. This is evident in their active involvement in the biometric ID card issue and, to some extent, the Safe City project. This exemplifies how sustained civic engagement can successfully influence political decision-making, particularly on issues concerning privacy and surveillance. Their efforts have, hopefully, led to lasting changes in state intelligence policy and practice.

References

Abebe, M. 2018. Africa's Security Landscape: Counterterrorism and Surveillance. *Journal of African Security Studies.* pp. 4, 23-45.

AccessNow et al. May 2021. Joint civil society statement in response to the Information & Telecommunications Authority Consultation paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of social media in Mauritius. *AccessNow.*

[34] Nam News Network (2021) Mauritians call on the government to resign in mass protest. Retrieved at http://www.namnewsnetwork.org/?p=113460, accessed 2 February 2024.

[Online]. [Accessed 20 December 2022]. Available from: https://www.accessnow.org/wp-content/uploads/2021/05/Mauritius-ICT-Act-Submission.pdf.

Acemoglu, D. and Robinson, J.A. 2012. *Why Nations Fail: The Origins of Power, Prosperity, and Poverty.* London: Profile Books.

Akech, M. 2009. The African Security Regime and the 'War on Terror': Developments, implications and prospects. In: Ahluwalia P. et al. eds, *Violence and Non-Violence in Africa*. London and New York: Routledge.

Allen, R. 1999. *Slaves, Freedman and Indentured Labour in Mauritius*. Cambridge: Cambridge University Press.

Baichoo, S. et al. (2018) Legal and ethical considerations of biometric identity card: Case for Mauritius, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, https://www.sciencedirect.com/science/article/abs/pii/S0267364918301535?via%3Dihub.

Bertelsmann Stiftung. 2024. Mauritius Country Report: BTI 2024. *BTI Transformation Index.* [Online]. [Access 2 July 2024]. Available from: https://bti-project.org/en/reports/country-report/MUS.

Birkland, T. 1997. *After Disaster: Agenda Setting, Public Policy, and Focusing Events*. Washington, DC: Georgetown University Press.

Brown, D. 2020. Biometrics and Surveillance: The Use of Biometric Technology by African Governments. *African Journal of Technology and Society*. 15(2), pp. 109–25.

Bunwaree, S. 2001. Mauritius: Democracy and Development in a Plural Society. *The Round Table: The Commonwealth Journal of International Affairs*. 90(360), 415–28.

Bunwaree, S. and Kasenally, R. 2005. *Political parties and democracy in Mauritius*. EISA Research Report No. 19.

Chan-Meetoo, C. 2021. *Analytical Paper on the ICTA Consultation Paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius*. [Online]. [Accessed 28 February 2023]. Available from: https://www.christinameetoo.com/wp-content/uploads/2021/05/20210519-Assessing-the-proposed-amendments-to-the-ICT-Act-C-Chan-Meetoo.pdf.

Chenganna, A. 2022. *Popular talk radio and everyday life in Mauritius*. PhD Thesis, University of Cape Town.

Cormack, D. and Kukutai, T. 2022. Indigenous Peoples, Data and the Coloniality of Surveillance. In: Hepp, A. Jarke, J. and Kramp, L. eds. *New*

Perspectives in Critical Data Studies: The Ambivalences of Data Power. Cham: Palgrave Macmillan.

Couldry, N. and Yu, J. 2018. Deconstructing datafication's brave new world. *New Media & Society*. 20(12), 4473–91.

David, A. and Petri, M. 2013. Inclusive Growth and the Incidence of Fiscal Policy in Mauritius – Much Progress, But More Could Be Done. *IMF Working Paper No. 13/116*. Washington, DC: International Monetary Fund.

Duncan, J. 2018. Activist Learning and State Dataveillance: Lessons from the UK, Mauritius and South Africa. In: Choudry, A. ed. *Activists and the Surveillance State Learning from Repression*. London: Pluto Press.

Duncan, J. 2022. *National Security Surveillance in Southern Africa: An Anti-Capitalist Perspective*. London, New York, Oxford & New Dehli: Zed.

Fillieule, O. and Accornero, G. eds. 2016. *Social movement studies in Europe: The state of the Art*, vol. 16. New York: Berghahn Books.

Gadzala, A. 2018. Surveillance and the Security State in Sub-Saharan Africa. *Global Security Review*. 5, pp. 82–96.

Giugni, M. 2009. Political opportunities: From Tilly to Tilly. *Swiss Political Science Review.* 15(2), pp. 361–8.

Gunner, L., Ligaga, D. and Moyo, D. (eds). 2012. *Radio in Africa: Publics, Cultures, Communities*. Rochester, NY: James Currey.

Herweg, N., Zahariadis, N. and Zohlnhöfer, R. 2022. Travelling Far and Wide? Applying the Multiple Streams Framework to Policy-Making in Autocracies. *Polit Vierteljahresschr.* 63, pp. 203–23.

Higley, J. and Burton, M.G. 2006. *Elite Foundations of Liberal Democracy*. London: Rowman & Littlefield Publishers.

Houbert, J. 1981 Mauritius: Independence and Dependence. *The Journal of Modern African Studies*. 19(1).

Jahangeer-Chojoo, A. 2010 From Minority to Mainstream Politics: The Case of Mauritian Muslims. *Journal of Social Sciences*. 25(1–2–3), pp. 121–33.

Kasenally, R. 2011. Mauritius: The not so perfect democracy. *Journal of African Elections*, 10(1), pp. 33–47.

Kasenally, R. 2022a. The Trappings of the Mauritius Safe City Project. *The Hoover Institution*. [Online]. [Accessed 18 December 2023]. Available from: https://www.hoover.org/research/trappings-mauritius-safe-city-project.

Kasenally, R. 2022b. Is Digitalisation Endangering Democracy in Mauritius? In: Kerley, B., Kasenally, R., Simão, B. and Santos, B. eds. *Smart Cities and Democratic Vulnerabilities*. National Endowment Fund & International Forum for Democratic Studies. [Online]. [Accessed 22 April 2024].

Available from: https://www.ned.org/wp-content/uploads/2022/12/Smart-Cities-and-Democratic-Vulnerabilities.pdf.

Kasenally, R. and Ramtohul, R. 2020. *The Cost of Parliamentary Politics in Mauritius. Westminster Foundation for Democracy*. [Online]. [Accessed 21 February 2024]. Available from: https://www.wfd.org/sites/default/files/2022-01/Cost-of-Parliamentary-Politics-in-MauritiusWEB-FINAL.pdf.

Kingdon, J. 1995. *Agendas, Alternatives, and Public Policies*. 2nd Edition. Boston: Addison-Wesley Longman Inc.

Kingdon, J. W. (1995). Agendas, Alternatives, and Public Policies (2nd Ed.). Longman, MI: The University of Michigan.

Kumar, B.N. 2019. Societal Expectations of Good Governance: Case Study on Mauritius. *Irish Interdisciplinary Journal of Science & Research*. 3(2), pp. 01–09.

Leon-Espinoza, D. (2022). Explaining the adoption of care policies in Costa Rica and Uruguay: A multiple streams approach. Social Politics, 29(4), 1379-1402.

Lyon, D. 2009. *Identifying Citizens: ID Cards as Surveillance*. Cambridge and Malden: Polity Press.

Maurer, S. 2015. Mauritius: Culture Crossings and its Consequences. *Antrocom Journal of Anthropology*. 11(1).

McAdam, D., McCarthy, J.D. and Zald, M.N. eds. 1996. *Comparative perspectives on social movements: political opportunities, mobilising structures, and cultural framings*. Cambridge: Cambridge University Press.

Mehta, R. 2015. Ethnicity, Ethnic Relations, and Development of Mauritian Society. *Indian Anthropologist*. 45(1), pp. 47–60.

Murday, L. 2023. Mauritius: Moving Towards Mass Surveillance. In: Shaffer, R. ed. *The Handbook of African Intelligence Cultures*. London: Rowman & Littlefield.

Mwesiga, D. 2021. *Mauritius' Social Media Regulation Proposal Centres State-Led Censorship. CIPESA*. [Online] Available from: https://cipesa.org/2021/05/mauritius-social-media-regulation-proposal-centres-state-led-censorship/ accessed on 20 December 2022.

Mwesiga, D (2021) *Mauritius' Social Media Regulation Proposal Centres State-Led Censorship*. CIPESA. Retrieved at https://cipesa.org/2021/05/mauritius-social-media-regulation-proposal-centres-state-led-censorship/ accessed on 20 December 2022

Phaahla, E (2019) Mauritius' Competitive Party Politics and Social Democratic Welfare Outcomes after Independence. *Strategic Review for Southern Africa*, Vol 41, No 2. Nov/Dec 2019

Phaahla, E. 2019. Mauritius' Competitive Party Politics and Social Democratic Welfare Outcomes after Independence. *Strategic Review for Southern Africa*. 41(2).

Phoker, A. 2021. Mauritius Must Not Fall into the 'Mass Surveillance' Trap. [Online]. [Accessed 17 November 2023]. Available from: https://www.internetsociety.org/blog/2021/05/mauritius-must-not-fall-into-the-mass-surveillance-trap/

Ramtohul, R. 2018. Mauritius: Still a long journey ahead. In: *The Palgrave Handbook of Women's Political Rights*. pp. 547–561. London: Palgrave Macmillan.

Ramtohul, R. 2021. Diaspora and development: the case of Mauritius, *Development in Practice*, 31 (6), pp. 828–38.

Ramtohul, R and Hylland E (2018) *The Mauritian Paradox: Fifty years of Development, Diversity and Democracy*. African Books Collective.

Shaffer, R (2021) (ed) *African Intelligence Services: Early Postcolonial and Contemporary Challenges*. Rowman & Littlefield

Schmidt, E. 2013. *Foreign Intervention in Africa: From the Cold War to the War on Terror.* Cambridge: Cambridge University Press.

Shaffer, R. 2021. *African Intelligence Services: Early Postcolonial and Contemporary Challenges*. London: Rowman & Littlefield.

Sithanen, R. 2003. *Coalition politics under the tropics: office seekers, power makers, nation building: A case study of Mauritius*. As presented at an EISA Roundtable Political party coalitions – Strengthening Democracy through Party Coalition Building. Vineyard Hotel, Claremont, Cape Town, 19 June 2003.

Srebrnik, H. 2000. Can an ethnically based civil society succeed? The case of Mauritius. *Journal of Contemporary African Studies*. 18(1), pp. 7–20.

Tarrow, S. (1998) Power and movement: Social movements and contentious politics. Cambridge University Press, Cambridge

Tarrow, S. 2011. *Power in movement: social movements and contentious politics.* Revised and updated, third edition. Cambridge: Cambridge University Press.

Walby, K. and Hier, S. 2009. Risk Technologies and the Securitization of Post-9/11 Citizenship: The Case of National ID Cards in Canada. *Socialist Studies/Études Socialistes* 1(2), pp. 7–31.

CHAPTER SIX

Surveillance as a mechanism of political control in Mozambique: The structural environments for the failing of public oversight mechanisms

Ernesto Nhanale and Borges Nhamirre

Introduction

Recognising that intelligence services are crucial for preventing threats to state security, and that they must operate within principles of accountability and legitimacy – especially in a democracy – this chapter aims to examine the systematic weaknesses in the oversight mechanisms of Mozambique's intelligence services. The chapter starts by exploring the historical context of the establishment of state intelligence services, marked by the legacy of the Portuguese colonial fascist regime, which relied on the International State Defence Police (PIDE) as its operational arm and the installation of the National Popular Security Service (SNASP). Subsequently, it discusses surveillance against those who fought authoritarianism. Furthermore, it examines the role the subsequent military conflicts played as elements in understanding the configuration, role and limitations of the current State Intelligence and Security Service (SISE), which was established in 1991 within the democratic framework (Zeca, 2021).

The central argument in this chapter is that there are low levels of oversight of the activities of the intelligence services, the SISE, and as a result, this leads to the perpetuation of its secret operating model, including its involvement in surveillance scandals and violations of citizens' fundamental rights. This situation arises from several factors. First, the activities of the intelligence services are governed by lenient laws that lack clear definitions of SISE's accountability. Second, the Head of State has excessive powers, giving them direct control over the intelligence agency as the Commander-in-Chief of the Defence and Security Forces. Third, the ruling party, the Mozambique Liberation Front (FRELIMO), is dominant and controls parliament and other state sectors. Additionally, the judiciary has a low level of independence, and there is a decline in the freedoms of expression and civic space overall.

Mozambique has experienced several incidents of surveillance, taking as a case study, the regulations requiring the registration of Subscriber Identity Module (SIM) cards in 2010, which was updated in 2024 to biometric registration. The success of these government initiatives, which reinforce the spaces for exercising surveillance in the digital context, is only possible due to limitations, a lack of skills, and knowledge of the supervisory institutions. As a result, the success of these initiatives increasingly reinforces a state of authoritarian democracy, keeping SISE at a level where it fulfils both its statutory functions and political surveillance operations in the interests of the Head of State, who is also President of the ruling FRELIMO party.

This article is centred on the external level of intelligence oversight, considering how the three functional levels – judicial oversight carried out through the courts, legislative oversight carried out through parliament and public/civil oversight carried out through civil society and the media performance in Mozambique and how they are influenced by the political authoritarian regime on their role of overseeing intelligence (Graves, 2018; Georgiev, 2022). The chapter also addresses the fact that to better evaluate the effectiveness of oversight mechanisms, it is important to understand the level of autonomy from security agencies and the government to have a greater capacity to scrutinise and demand the purpose for which surveillance activities are carried out (Raab, 2017). The oversight mechanisms vary from state to state and are influenced by historical, constitutional, legal and political culture factors (Bochel and Defty, 2017).

Methodologically, the chapter used a qualitative approach to data collection, relying on bibliographical and documentary research. On the documentary side, extensive use was made of the legal diplomas that regulate the intelligence service in Mozambique, from their origins in the period of the liberation struggle, through the one-party regime of the post-independence era, to the current period of multi-party democracy. Reports of the parliamentary commission of inquiry were also consulted on oversight of the defence and security sectors, including the intelligence services.

The effects of political authoritarianism on the oversight mechanisms of the intelligence services in Mozambique

Despite being formally a democratic state since 1990, Mozambique exhibits a hybrid political system that combines elements of both democratic and autocratic regimes. This fusion stems from the fact that, while the country possesses a democratic constitution and regularly holds elections, FRELIMO is the same political party that consistently is declared the winner of these elections, which are regarded as highly manipulated to perpetuate the ruling party in power (Hanlon, 2021; Do Rosário and Guambe, 2023). Additionally, Mozambique has limited respect for political freedoms, political rights, human rights, participation and transparency (Nhanale, 2019). Authors such as Levitsky and Way (2002, p. 52) call these models 'electoral dictatorships', 'semi-democracies', 'virtual democracies', 'electoral democracies', 'pseudo democracies', 'illiberal democracies', 'semi dictatorships' and 'light dictatorships', highlighting the collusion of certain elements of democracy and authoritarianism in the respective regimes (Gilbert and Hohseni, 2011).

Mozambique's hybrid political system, characterised by elements of both authoritarianism and democracy can be attributed to three historical factors: the fascist colonial heritage; the 10-year national liberation struggle, which was the cradle of the Mozambican defence and security forces, including the intelligence services; and the legacy of a one-party authoritarian regime adopted by the Mozambique Liberation Front shortly after political independence. In 1975 Mozambique became independent from Portugal, which since 1933 had been ruled by a fascist dictatorship that came to an end through a military revolution of 25 April 1974 (Furtado, 1997/1998, pp. 204–5). The use of surveillance in the former colonies through the PIDE was one of the driving forces behind its success and the longevity of Salazar's Estado Novo regime in Portugal (Sirrs, 2021).

In addition to the fascist colonial regime, it is also important to consider the period of the war of Mozambique: a quarter of a century of war and 10 years for the national liberation struggle. These were the cradle of Mozambique's Defence and Security Forces, including the intelligence services, as they were shaped and moulded during the 10-year national liberation struggle, which was waged by FRELIMO against the Portuguese colonial state. They are, therefore, services moulded in the military context of a liberation movement that is unlikely to shed its historical origins.

Two years after its political independence, Mozambique in 1977 transitioned into an authoritarian state at the Third Congress of the FRELIMO party. At this gathering the party officially adopted a Marxist-Leninist and 'vanguard' ideological orientation, leading the country towards a single-party state (Do Rosário, 2024). The implementation of Marxism-Leninism had varied effects, particularly in terms of limited opportunities of political rights and civil liberties. These restrictions were only formally abandoned, at least, following a civil war led by the Mozambican National Resistance (RENAMO), an opposition group that vehemently opposed the state's totalitarian regime (Cabrita, 2000). The Mozambican State Intelligence Services (SNASP) was established through Decree No 21/1975. It adopted the structure that had already existed during the national liberation struggle, which included intelligence units, such as the Department of Defence and Security along, with control or accountability models (Zeca, 2021, p. 232).

Of the three objectives defined for the SNASP's mandate, the third focuses specifically on surveillance issues: 'to prevent and neutralise all espionage activities aimed at undermining the national unity of the country'. According to article 5 of Decree 21/1975, these powers include seizing mandates and detaining individuals to be sent to re-education camps. To fulfil its role the SNASP was granted police powers and arbitrary authority to act, and reported directly to the President of the Republic and at the same time to FRELIMO. The Decree further solidified SNASP's authority by mandating to serve as the umbrella of the National Migration Services.

The political model adopted by FRELIMO, the so-called *Xiconhocas*, marked an era and a clear policy of repression and control over civic space and freedom rights, which later degenerated into mistrust and internal political protests. As Nhanale (2021) points out, to put the policy of repression into practice, through the various forms of punishment of the so-called enemies of FRELIMO's post-independence revolutionary cause, it was important to monitor permanently the possibilities and actions seen as subversive. Surveillance emerged as a clear instrument of the authoritarian regime to deal with the various protest movements that took on violent forms in the capital, Maputo, and its suburbs. Concurrently, the government conflict with RENAMO, which had the support of the Rhodesian regime through the Central Intelligence Organisation (CIO) and the Apartheid regime through South Africa's Bureau of State Security (BOSS) also inevitably accelerated the intensification of mass control-actions to better identify enemies (Machava, 2011).

Amidst the escalating external hostilities against Mozambique, particularly from the Apartheid regime and Southern Rhodesia, and with the support of the Central Intelligence Agency (CIA), the Mozambican government introduced the law on crimes against people and people's security in 1979. This law aimed to safeguard national security against imperialist attacks. It broadened the scope of internal and external targets suspected of committing crimes against state security. These amendments granted the SNASP more discretionary authority, including capturing political opponents and transferring them to the so-called 're-education camps' in Niassa Province. Additionally, some individuals were subjected to torture or tried in popular tribunals established by the same law, without oversight by the courts.

The excessive powers and abuses granted to the SNASP were acknowledged by the Mozambican government, which initiated a campaign in 1981 to curtail these excessive powers and abuses (Sirrs, 2021; Bussotti and Nhaueleque, 2023)

Although FRELIMO decided during its fifth congress in 1989 to make a nominal change from SNASP to SISE, the process of transforming SNASP into a professional state security service only began shortly after the introduction of the 1991 Democratic Constitution (Law 20/91). SISE was created just before the 1992 General Peace Agreement between the government and RENAMO, hence its principal focus remained on war-related concerns. RENAMO, as a surveillance target, remained a priority for the security services, resulting in actions that stretched into the democratic period in an attempt to curb the group's political activity.

Despite this new structure, SISE remains under the direct control of the Head of State, operating with high levels of secrecy. Its Director General was given extra responsibilities by Decree 8/93, allowing them to chair the National Committee for the Implementation of the Norms on State Secrets, which oversees all bodies concerned in state security problems. Laws 12/2012 and 13/2012 finalised the legal framework governing state security in response to the difficulties posed by the National Defence Strategy, which was approved by Resolution 42/2006.

From a supervisory perspective, these modifications have not greatly increased accountability for SISE's activities. The Director General of SISE is only obligated to present an annual report to the State Defence and Security Committee, which is mostly made up of security industry representatives. The intelligence services of modern Mozambique are the descendants, or mere continuations, of the intelligence agencies that existed under the one-party rule throughout the Cold War and civil war:

> The democratic states that have emerged in the post-Cold War international system as a result of the Third Wave of Democratisation often have intelligence and security services that are heirs or continuators of models that operated under dictatorships or one-party political regimes. These intelligence agencies' actions are inextricably related to the legacy of

> political and social repression imperatives, the dynamic contingencies of the Cold War, and internal disputes (Zeca, 2021, p. 382).

Even after the 1992 General Peace Accords ended the Mozambican Civil War, the country has continued to face military conflicts that necessitate strict control and surveillance. Mozambique has fought with numerous military confrontations, including Ian Smith's invasion from Rhodesia, attacks by the Apartheid state, and a protracted armed struggle that lasted 16 years, which reappeared between 2013 and 2016 owing to electoral discord from RENAMO. This lasted until 2019 with the signing of peace agreements and the demobilisation of RENAMO forces. Additionally, since 2017, Mozambique has been combating insurgents in the provinces of Cabo Delgado and Niassa, known as armed groups linked to the Islamic State (Ngoenha et al., 2020).

The 16 years of civil war ingrained a culture of conflict within the intelligence services, which has persisted in the post-conflict period as the actors involved in the war remain the same. For example, in 2015 Lagos Lidimo, who had led military counterintelligence throughout the civil war, was appointed Director General of SISE. He was raised in a combat environment; therefore, it is doubtful he could completely transition to a democratic intelligence service mindset. Lidimo is one well-known example, but several military officers from the civil war make up the command and operational organisation of SISE today.

As observed, the institutionalisation of the intelligence services in Mozambique reflects the state's political trajectory and has consistently aligned with the interests of the authoritarian regime dominated by the FRELIMO Party, both as the single party and as the dominant party in the context of electoral democracy. It has developed into a professional intelligence agency, but as long as the President of the Republic has authority, it will always be primarily focused on monitoring journalists, civil society and political rivals. Its operations are too complex for organisations like the parliament and the courts to effectively monitor.

Excessive presidentialism and regulation weakening the role of parliament and the judiciary

The legacy of authoritarian culture, FRELIMO's control of the state, and the extensive powers of the Head of State have undermined the separation of powers, resulting in a stronger executive and a diminished role for parliament and the judiciary. Legislative shortcomings in defining parliamentary and judicial monitoring systems aggravate these political issues.

According to Forquilha and Orre (2011, p. 41), FRELIMO's operation inside the dominant party system of Mozambique's multiparty era has resulted in complete control over the legislative and judicial branches, which has fostered intolerance, political exclusion and an institutional dependence on the ruling party. This has frequently had a negative impact on political involvement by leading to a lack of transparency, clientelism, corruption, electoral fraud, limited institutional legitimacy and the continuous operation of institutions based on a one-party system model (Nhanale, 2021).

Mozambique's first Constitution, enacted in 1975, stipulated that FRELIMO would direct all state entities and follow the concepts of unity of power, democratic centralism and dual subordination. The 1978 Constitutional Amendment gave the National Assembly (then known as the People's Assembly) limited legislative powers, with no authority to monitor the administration or the defence and security forces. Furthermore, pursuant to Article 47, the People's Assembly was convened and headed by the Head of State or at the request of the FRELIMO Central Committee and its Standing Committee, the members of which were elected based on FRELIMO Central Committee suggestions.

Thus, while the 1978 Constitutional Amendment gave Parliament legislative powers, it also preserved the FRELIMO Party's authority to oversee and monitor the acts of state agencies as a single party, to which the executive bodies reported.

Under the 1975 Constitution, the President of the Republic, who was also the President of FRELIMO, served as Head of State and Government, with absolute authority over the National People's Security Services, as well as the President and Vice-President of the Supreme People's Court and the Attorney General of the Republic, through his powers of appointment, assignment and dismissal. Although Article 75 entrusted the judiciary with the responsibility of ensuring compliance with laws and legal norms, it was not independent of the executive branch. It was managed by the President through the appointment of superiors. However, under Article 69 of the 1978 Constitution, these services were subordinated to the People's Assembly.

The 1990 Constitution and its 2004 amendment established the principles of democratic rule of law, multi-party politics, fundamental liberties for citizens and the separation of state powers – executive, legislative and judicial. From the point of view of the state bodies, the President of the Republic, although elected, continued to have a series of powers, as Head of State, Head of Government, and Commander-in-Chief of the Security Forces and Defences and, on the other hand, still has the power to appoint the Presidents of the Bodies of the Justice's Administration (Supreme Court, Administrative Court, Public Prosecutor's Office and the Constitutional Council). In addition to the respective, the Assembly of the Republic, which is made up of 250 elected members, has general oversight rights under Article 173, including the ability to request and collect information from the administration, as well as raise questions and interpellate the government. The Assembly of the Republic in the first instance has legislative authority over defence and security policy.

The SISE members are assigned a nonparty Statute. Article 20 of the SISE Members' Statute and Article 3 of the Regulation of Law 12/2012 of 2012 established the notion of nonpartisanship. However, Article 266 of the 1990 Constitution states that the defence forces and state security services owe special loyalty to the President of the Republic in his capacity as Commander-in-Chief, who is also the leader of the ruling party, FRELIMO. The figures of the Ombudsman and the National Defence and Security Council are introduced by the 1990 Constitution; however, both are unclear on questions of monitoring of the defence and security forces.

Decree 54/1975 and Law 20/91, the principles of the SISE's subordination and the services it provides directly to the President of the Republic have been far removed from the laws that founded it, and they are upheld by Law 12/2012 and its regulations.

Although Article 4(3) of the regulation generally establishes the competences of 'detecting in time signs of crimes against state security or of a transnational nature and activities that constitute a threat or potential threat to state security', Article 1 of the SISE regulation objectively establishes that the purpose of the scope of the services provided by the institution is to produce useful and strategic information for the President of the Republic on matters of national security. Given the political climate and the Head of State's party interests, this provision is problematic and can lead to political surveillance.

Another awkward aspect is that the concept of 'state security' in Mozambique has been hotly debated, particularly because Law 19/91, which defines it, is ambiguous, stating in Article 22 that defamation of the Head of State, ministers, Supreme Court judges, and even General Secretaries of political parties is considered a crime against state security, punishable by one to two years in prison. This means that, in the name of 'state security', regular individuals' communications might be demanded by state intelligence services when they criticise individuals protected by the aforementioned national security standard.

According to its regulations and governing law, SISE is required to work with the criminal investigation police, the Attorney General's Office and the courts to investigate criminal charges. The collaboration is facilitated by its authority to collect information and intercept communications. However, this poses various significant issues, particularly with regard to the regulation that provides SISE unrestricted access to citizens' data via network operators and service providers, as described in Article 8 of its regulation, namely clauses a) and b) as quoted below:

> Network operators and service providers have a duty to co-operate during the interception process required by SISE, and to this end, they must: a) make available interfaces and/or specific equivalent equipment enabling the interception of

> communications; b) allow the installation of devices and/or equipment defined by SISE for the purpose of carrying out the interception of communications.

This provision contradicts Law No. 4/2016, which, in Article 66, requires all telecommunications carriers to establish an effective and efficient system for intercepting communications for criminal investigation reasons, but only with the approval of a criminal investigating court. Two years before this law was passed, the government adopted Regulation 75/2014 on telecommunications traffic regulation. Similarly, the provision in Article 8 of the SISE regulation contradicts Law No. 03/2017, Article 14, which requires intermediate providers of data-transmission services to maintain the secrecy and confidentiality of all communications, prohibiting their disclosure without a judicial or administrative decision.

The same considerations apply to phone tapping. Article 222 of Law No. 25/2019, which adopts the new Code of Criminal Procedure, provides for the interception and recording of suspects' telephone calls or other electronic methods as evidence. This provision reinforces SERNIC's key role under Law No. 02/2017, which says in Article 21(a) that interception and recording of communications must be performed as part of a criminal investigation into suspects and must be authorised by the relevant judicial authority.

As can be seen, the constitutional and legal framework, as well as the institutional structure, severely constrain the courts' and parliament's ability to oversee SISE. To begin with, while there are general definitions of parliaments' and courts' oversight functions, these definitions are not specific to SISE's activities, nor does Law No. 12/2012, which created SISE, clearly specify accountability standards. Furthermore, the legal rules allow intelligence services to conduct intrusive activities with no obvious limits.

In the defence and security sectors, only the Ministers of the Interior and National Defence are held accountable by Parliament. At no point is the Head of SISE required to publicly answer to parliament.

Even though MPs have the authority to criticise the performance of the state sector and there is a parliamentary committee dealing with defence and security concerns, meetings with SISE to clarify pertinent concerns have never been made public.

In most democratic countries, parliaments are characterised as the legislative framework for intelligence supervision, in which Members of Parliament monitor the activities of security agencies. This exemplifies how elected authorities, who represent citizens, aim to ensure more accountability. Behind parliament, security organisations can be held more accountable for their operations, preventing autocratic use of surveillance laws while also creating legal parameters for security issues and ensuring a balance between security and fundamental freedoms (Born and Fluri, 2004). According to Born (2004, p. 136), 'Parliament plays an important role in safeguarding the democratic element of overseeing the security sector.'

In Mozambique, FRELIMO's parliamentary dominance undermines its function for effective oversight, because, as previously stated, SISE is an important body not only for state security but also for providing surveillance services to the Head of State, who has political interests as President of the FRELIMO Party. This is a domineering effect, reducing the body's ability to exercise supervisory functions over SISE.

One typical instance is the 'hidden debts' scandal that topped off in 2016, the country's most significant secret debt scandal, involving projects related to the defence and security sectors, under which Armando Guebuza's government is said to have incurred debts of approximately 1.5 billion United States dollars for investments in the maritime security sector and in companies related to mineral resource exploitation (Nhanale, 2019). These debts, contracted without consulting or informing parliament, were viewed as a violation of democratic institutions and resulted in the arrest, trial and conviction of senior SISE figures, including the Director of Economic Intelligence Services and the Director General.

Mozambique's undue secrecy scandal exemplifies the degree to which the culture of secrecy is ingrained in public administration, as well as the consequences of controlling supervisory institutions and the Head of State's disproportionate powers over the government and the defence and security services. This secrecy has also been linked to mistrust and the belief that RENAMO, as an opposition group, is still an adversary to be defeated. For, according to the former President of the Republic, Armando Guebuza, as he testified in court, the process was not subject to parliamentary oversight, because the purpose of the project that was going to be financed was state security, and, in parliament, RENAMO was an enemy of the state, especially at a time when its leader, Afonso Dhlakama, was in the Gorongosa forests, in the centre of Mozambique, leading a military insurrection in claiming the previous election result.

Weak public oversight through the media and civil society

Civil society advocates for accountability and strategic litigation, and the media acts as a watchdog, investigating excesses and abuses by intelligence organisations (Bochel and Defty, 2017). As Georgiev (2022, p. 31) points out, civic oversight mechanisms can be 'implemented through the activity and exercise of rights (access to information, complaints and signals, requests, opinions and proposals, expression) by citizens, media, and NGOs is an important mechanism implemented in several democratic countries with the aim of promoting greater efficiency and citizen participation, both in legal and institutional reforms, as well as in education, information and the production of knowledge about the relevance of democratic approaches to intelligence sectors' (Caparini, 2004).

When considering the role of civil society (non-governmental organisations (NGOs) and the media), two key elements are critical for understanding their role in overseeing intelligence services: first, the extent to which these freedoms are exercised, both legally and practically; and second, the technical capacity for research, knowledge production, monitoring and advocacy for public policies.

This analysis of civil society organisations and the media's role in intelligence oversight takes these two components into account. It demonstrates that, while laws allow for the exercise of free expression, press freedom and the operation of civil society organisations significant legal limits limit their efficacy as supervisors of government institutions on a variety of topics. This includes the government's proclivity to enact policies that limit civic space. Furthermore, it argues that effective monitoring of intelligence services necessitates a high level of technical expertise and specialisation. While some civil society organisations pursue similar activities, their efforts are frequently hampered by a lack of specialisation and technical expertise.

Authoritarian culture and restrictions on civic space

With the advent of democracy, the 1990 Constitution allowed for the introduction of civil and political freedoms, as regulated by the Press Law (Law 18/91), the Political Parties Law (Law 07/91), the Associations Law (Law 08/91), the Freedom of Assembly and Demonstration Law (Law 9/91), and the Right to Information Law (Law 34/2014). This legal framework formalises the establishment of a democratic public sphere in Mozambique.

Despite the fact that these principles provide a democratic public sphere in which the media and civil society can operate, they have several restrictions. Low levels of development, poverty and illiteracy all have an impact on literacy rates and, consequently, access to information. These factors have contributed to what scholars such as Shenga and Mattes (2009) refer to as an 'uncritical citizenship culture', which is defined by high levels of citizen trust in leaders, even when institutions demonstrate little commitment to democracy.

Even in this limited climate, the media, civic society and individuals have expressed a desire for transparency and improved public services. This is especially visible in major cities like Maputo, where high levels of urban poverty, persistent corruption and a lack of inclusive public policies that serve individuals' needs have resulted in widespread unhappiness. In other cases, this unhappiness has resulted in violent protests and popular opposition to government policy (Pereira and Nhanale, 2014, pp. 3–5).

The concept of uncritical citizenship dominates Mozambique's civic culture, especially when examining the historical forces that influenced participation and freedoms in the state-building process.

Examples include the political and cultural attitudes of subjugation fostered during the colonial era, the culture of fear instilled throughout the 16-year war and the one-party political system implemented following national independence. These characteristics have helped to create an uncritical culture (Shenga and Mattes, 2009). The authoritarian political culture founded in FRELIMO's historical vision of state and party control as faithful interpreters of citizens' interests severely limits the scope for supervisory activity by the media and civil society (Macamo, 2014).

The shrinking of spaces for freedoms, along with pressure to use these freedoms in monitoring the executive's actions, has resulted in the perpetuation of authoritarian methods such as the surveillance of journalists and civil society activists. This surveillance is a crucial tool of political intolerance, persecution and physical violence against journalists and opinion makers criticising FRELIMO's rule (Sirrs, 2021; Bussotti and Nhaueleque, 2023).

This surveillance serves as a technique for controlling public opinion within institutionalised settings, particularly the main public media, as well as impeding the functioning of civil society organisations that may question government policy. Monitoring data on freedom of speech and the press in Mozambique demonstrates that journalists continue to face violations, including arbitrary arrests, kidnappings and even murders, throughout the democratic process. Furthermore, the country has seen legislative initiatives aimed at limiting civic space and introducing more surveillance mechanisms, such as proposed changes to the Media Law, the Law on Civil Society Organisations and the Law on Combating Terrorism and Money Laundering (MISA-Mozambique, 2021–3; Nhanale and Cossa, 2024).

These measures supplement existing laws that have been identified as restrictive to civic space, including the State Secrecy Law (Law No. 12/79), which has not been repealed and imposes excessive limitations on the definition of secrecy, contradicting freedoms of expression, and the Penal Code (approved through Law No. 35/2014, of 31 December), which criminalises defamation of senior state figures and political leaders as a crime against state security (FES and MISA, 2018).

Low capacity and expertise of the media and NGOs in oversight

While the media and civil society organisations benefiting from constitutionally protected freedoms conduct significant oversight activities, their efforts remain very limited in the defence and security sectors, and almost non-existent in the intelligence sector, in particular. These constraints are related to a lack of institutional capacity and experience required for effective control, notably in the security industry.

Mozambique's civil society organisations have made significant contributions to government monitoring in social and economic sectors, such as health, education, natural-resource management, land and public finance (Forquilha and Gonçalves, 2022, pp. 25–6). However, civil society supervision has not focused on the governance of the defence and security sectors as a whole, particularly the intelligence sector. This is mostly due to two important considerations. First, the closed nature of this sector, whose acts are not in the public domain or, in cases where they are known to the public, are not thought to be those of the secret services, and second, civil society organisations' lack of knowledge in national security problems.

Mozambique's civil society organisations are frequently thematic, focusing on areas such as health, education, women and children, disabilities, democracy, human rights, media and natural-resource management. However, there is a distinct lack of organisations focused on the defence and security sector, particularly the intelligence sector.

The discovery of natural resources in Cabo Delgado, combined with the advent of violent armed conflict in the same province, spurred the government to expand security efforts in Cabo Delgado and dedicate more budgetary resources in response to the conflict. Some civil society organisations have started providing public consulting services in the defence and security sectors.

Since 2020, the Centre for Democracy and Human Rights (CDD) has been implementing a programme named 'The Voluntary Principles on Security and Human Rights in Mozambique'. The initiative, which works with the Geneva Centre for Security Sector Governance (DCAF), promotes communication and collaborative problem-solving to improve security and human-rights conditions for corporate investments in Cabo Delgado province. This programme has facilitated agreements between companies and security providers to reduce security and human-rights concerns, in line with the Voluntary Principles (VPs) (CDD, 2022, p. 2).

Although CDD's Voluntary Principles programme brought together leaders from the defence and security sectors, security-service providers and multinational corporations based in Cabo Delgado, this activity does not constitute public oversight of the defence and security sector or intelligence services. Instead, it is mainly focused on monitoring human-rights violations by private security-service providers engaged by multinational corporations that exploit natural resources.

The Centre for Public Integrity (CIP), a Mozambican civil society organisation that monitors government and combats corruption, has overseen the entire defence and security sector. Since the onset of the conflict in Cabo Delgado, CIP has undertaken various studies to monitor the defence and security sector, although these are primarily econometric analyses aimed at examining defence and security spending during the conflict, the accountability of such spending, rather than the sector's operational issues and respect for individual liberties.

CIP's 2021 study, 'External Control of Defence and Security Expenditure: How Much Does the State Spend on the War in Cabo Delgado and How Does It Spend It?' concluded that the war in Cabo Delgado had cost more than 64.77 billion meticais ($1.1 billion) over three years (2017–19), with official security and defence spending tripling from 21 billion meticais to 62 billion meticais annually. The analysis identified a lack of accountability in military spending during the Cabo Delgado conflict (Bande and Constantino, 2021, p. 8).

In 2023, CIP undertook another analysis to examine the financial impact of the Cabo Delgado battle, discovering a significant rise in national-security expenditures from 2018 to 2022, totalling an estimated 106.8 billion MZN (1.69 billion USD) (CIP, 2023).

The CIP's studies appear to be primarily related to the ongoing war in Cabo Delgado and so are not the outcome of normal monitoring of state security services. Although these studies monitor the defence and security sectors as a whole, including the State Intelligence and Security Service, their concentration is on budget utilisation rather than an overall assessment of the agency.

Beyond the CDD and CIP's activity, nothing is known regarding civil society's public examination of state security services. This lack of information is not owing to a lack of issues to monitor, but rather to two major factors: the undemocratic atmosphere, which limits security-service monitoring and the media's and civil society organisations' inadequate skill in conducting such audits.

One of the key factors contributing to the limited expertise of the media and civil society organisations in overseeing the intelligence services in Mozambique is the legal framework that makes intelligence activities exclusively the domain of the state. This means that anyone who has legitimately conducted intelligence work has done so in the service of the state. Furthermore, the law states that intelligence officers do not retire; after completing their mission, they are placed on reserve but remain legally tied to the intelligence services. This legal linkage makes it difficult for them to establish civil society organisations or media groups to scrutinise the very state they have served or continue to serve.

The impact of weak oversight bodies and surveillance incidents

As previously discussed, Mozambique's intelligence agencies have a history of abusive surveillance, owing mostly to the absence or weakness of control procedures. Numerous scandals have been documented throughout history, including frequent human-rights violations, political persecution that resulted in arbitrary incarceration, torture and murder in the 1980s (Amnesty International, 1985). These crimes were followed by attacks on political opposition members, as well as surveillance and wiretapping of civil society activists and journalists throughout the next decade (Sirrs, 2021; Bussotti and Nhaueleque, 2023).

In recent years, Mozambique has seen tremendous investment in surveillance technology. In 2014, ZTE Corporation, a telecommunications company, launched a project to install a system that would improve the ability to intercept and monitor citizens' communications by constantly reading messages (SMS, emails, WhatsApp and Viber), tapping phones and monitoring social networks and websites. This project involved the installation of 450 high-definition cameras and real-time data transmission for public surveillance on important roadways in Maputo and Matola, as well as parts of National Road 1 (Tsandzana, 2016; Caldeira, 2018).

In 2016, an investigative magazine published documents suggesting that ZTE Corporation, a telecommunications company, launched a project to install a system that would improve the ability to intercept and monitor citizens' communications. According to the report, ZTE told government officials that the system was capable of reading messages (SMS, emails, WhatsApp and Viber), tapping phones and monitoring social networks and websites.

One instance that deserves special emphasis in this research is the regulation of SIM-card registration in Mozambique, which was implemented in 2010 through Ministerial Diploma 153/2010. This approach required SIM-card holders to register, and unregistered numbers were prohibited. According to the government, the goal of this rule was to encourage responsible SIM-card use while also contributing to the maintenance of public order and tranquillity.

This measure is being implemented 13 years after the launch of mobile-phone services in Mozambique. The controversy surrounding this legislation originates from the fact that it comes after three successive civic rallies held by national residents, primarily in Maputo, in protest of living conditions, particularly rising food and fuel prices. There was a consensus that mobile phones and SMS played a major part in publicising the Maputo demonstrations in February 2008, September 2010 and November 2013.

As the demonstrations constituted a clear affront to an authoritarian government and, in the context of new technologies, the government, to allow greater surveillance and control of citizens, introduced the regulation for the registration of SIM cards. The Council of Ministers issued Decree 18/2015 in December 2015, which regulates the registration and activation of SIM cards. It was justified by Mozambique's telecommunications regulating authority, citing the need to defend national-security interests and combat crime. However, there were reasons for political control, collective monitoring and improper individual wiretaps (INCM, 2017).

As part of the developments in technology, these decrees were updated and improved. In 2023, the government revoked the previous decree on SIM-card registration, introducing Decree 13/2023 of 11 April, which regulates the registration process of telecommunications service subscribers to be observed by service operators, their distribution agents and/or resellers, public entities, private entities and individuals who own and use communication devices based on telecommunications services.

The Mozambican National Institute of Telecommunication (INCM), as cited by Jornal O Pais Online on 22 May 2023, stated that the effects of these surveillance adjustments were as follows:

> We want to ensure that every individual using a service on the country's telecommunications network is identifiable, that we are able to track them, and that we are certain the operation is being conducted by the correct person. Under the old regulation, we only registered the SIM cards, but now we register the subscriber themselves, the card, the device the subscriber will use, and the agent themselves (Nhanale, 2024, p. 12).

This intention is clearly concerning from the standpoint of its effects on undue surveillance, in a context where the laws do not establish any mechanism for data protection and oversight over data holders. The country's lack of a personal data-protection law, as well as laws that allow for the abusive use of surveillance, such as Laws 12/2012 and 13/2013; Articles 18 and 9 of the new Telecommunications Law (Law number 4/2016), as well as Article 14, number 4 of the same law; and Article 15 of the Communications Regulatory Authority's Law (No. 4/2021), are critical factors in these instruments' ability to reinforce surveillance.

This means that the data to be collected in biometric form will not be protected and will not be subject to oversight by bodies such as the courts, parliament, civic organisations and the media, all of which have flaws. Furthermore, the legal structure that established the INCM, which places it under the government's control in an authoritarian atmosphere, indicates the immediate risks of these policies.

These measures are not only concerning because of the risks they pose in facilitating undue digital surveillance, but also because of the lack of transparency with which they were implemented, as matters limiting fundamental rights were approved without prior consultation, whether through citizen participation or even parliamentary consultation. This is a measure that uses the potential of new technologies to expand the logic of control and restriction of civic space within political authoritarianism, while also exploiting the legislative permissiveness of wiretap policies to increase the capacity for abusive surveillance of citizens, journalists and activists.

Even though CIP attempted to advocate for the government's measure in 2010 and MISA Mozambique is currently doing some advocacy work on biometric regulation, these activities have had little impact owing to the organisations' limitations in terms of expertise and continuity of work. Furthermore, these government projects receive little media coverage and parliamentary oversight (CIP, 2010; MISA, 2024).

Conclusion

Throughout the chapter, it has been demonstrated that Mozambique has been ruled by an authoritarian regime since its independence, with restrictions limiting political freedoms in place. This implied the implementation of strict surveillance methods, not just for criminal concerns, but also for the control of persons deemed to be opponents of the Party-State.

Even in a democratic framework, Mozambique has encountered a number of security challenges, ranging from post-election political instabilities that prompted RENAMO to strive to transmit its claims through armed conflict to the current jihadist violent extremism in Cabo Delgado province. Even if they required the legitimate use of surveillance, these episodes, in the context of the country's political authoritarianism, have reinforced the culture of excessive surveillance, in a context where the adversary was defined not only in terms of the risks of military conflicts, but also political ones.

The authoritarian histories of Mozambique's institutionalisation of security agencies have left a legacy of poor transparency and accountability for their operations. Even though they operate in a democratic context, their institutional arrangement, which places their response and dependence on the Head of State, combined with excessive powers over their operations and the lack of clear legal mechanisms of accountability, makes their operations even more secretive, putting privacy and the use of technologies for abusive surveillance at risk. This effect is exacerbated by the existence of laws or sections of laws that violate freedom principles, as well as the lack of data-protection legislation, which allows law proposals that encourage abusive surveillance activities to be more successful.

These components demonstrate that democracy in Mozambique is primarily about formal or procedural matters, rather than establishing itself via the effectiveness of practices, particularly given that it remains a state with institutions that perpetuate an authoritarian ethos. The same party that led during the single-party rule continues to lead, relying on the same practices and leadership expectations, rendering institutions resistant to democratisation. One of the key issues that persists in Mozambique's democratisation discussion is the need not only for change, but also for state institutions to become more professional and freer of the single-party ethos.

The ongoing legal-reform process, instead of professionalising and reducing spaces for abusive surveillance, due to the fragility of oversight institutions – the parliament, judiciary, civil society and media – has been stimulating a reverse path, increasingly reinforcing surveillance spaces. The SIM-card registration regulation effectively grants regulatory authorities and telecommunications firms complete authority to gather citizens' data in bulk, with no control mechanism in place.

The lack of oversight is due, on the one hand, to the absence of an enabling environment for non-state entities to oversee intelligence-service activities and, on the other hand, to a lack of expertise on the part of the media and civil society organisations to oversee intelligence services, which stems largely from the past and authoritarian culture legacy.

The analysis produced throughout the chapter allows us to conclude that the suspected and upheld surveillance activities carried out by SISE in Mozambique, beyond the goals of safeguarding state security, may be used many times for political purposes and to restrict fundamental freedoms.

References

Bande, A. and Constantino, L. 2021. External Control of Defence and Security Expenditure: How much does the State spend on the war in Cabo Delgado and how does it spend it? [Online]. *CIP – Centro de Integridade Pública*. [Accessed 29 July 2024]. Available from: https://www.cipmoz.org/wp-content/uploads/2021/08/How-much-does-the-State-spend-on-the-war-in-Cabo-Delgado-and-how-does-it-spend-it-1-1.pdf.

Bochel, H. and Defty, A. 2017. Parliamentary Oversight of Intelligence Agencies: Lessons from Westminster. In: Neal, A.W. ed. *Security in a Small Nation – Scotland, Democracy, Politics*. Cambridge: Open Book Publishers, pp. 103–23. [Online]. [Accessed 29 July 2024]. Available from: https://www.openbookpublishers.com/books/10.11647/obp.0078.

Born, H. 2004. Learning from best practices of parliamentary oversight of the security sector: In: Fluri, P. and Hadžić, M. eds *Sourcebook on security sector reform: Collection of Papers. Belgrade*: Genorva: Geneva Centre for the Democratic Control of Armed Forces Centre for Civil-Military Relations, pp. 133–46. [Online]. [Accessed 29 July 2024]. Available from: https://www.dcaf.ch/sites/default/files/publications/documents/SSR_Democracy_Transnational_Societies.pdf.

Born, H. and Fluir, P. 2004. Oversight and guidance: The relevance of parliamentary oversight for the security sector and its reform. In: Fluri, P. and Hadžić, M. *Sourcebook on security sector reform: Collection of Papers*. Belgrade: Geneva Centre for the Democratic Control of Armed Forces Centre for Civil-Military Relations, pp. 123–31. [Online]. [Accessed 29 July 2024]. Available from: https://www.dcaf.ch/sites/default/files/publications/documents/SSR_Democracy_Transnational_Societies.pdf.

Bussotti, L. and Nhaueleque, L.A. 2023. Mozambique: Intelligence in the one-party culture of a democratic state. In: Shaffer, R. ed. *The Handbook of African Intelligence Cultures*. London: Rowman & Littlefield, pp. 461–71.

Cabrita, J. (2000) Mozambique: The Toruous Road to Democracy. Basingstoke, Palgrave.

Caldeira, A. 2018. Camaras de vídeo vigilância em Maputo e Matola são para distrair do comando de interceção de informação de Moçambique. Verdade, 4 April 2018. *Jornal Averdade*. [Online]. [Accessed 29 July 2024]. Available from: https://verdade.co.mz/camaras-de-video-vigilancia-em-maputo-e-matola-sao-para-distrair-do-comando-de-intercepcao-de-informacao-de-mocambique/.

Caparini, M. 2004. Civil society and democratic oversight of the security sector: A preliminary investigation. In: Fluri, P. and Hadžić, M. eds *Sourcebook on security sector reform: Collection of Papers*. Belgrade: Genorva: Geneva Centre for the Democratic Control of Armed Forces Centre for Civil-Military Relations, pp. 188–90. [Online]. [Accessed 29 July 2024]. Available from: https://www.dcaf.ch/sites/default/files/publications/documents/SSR_Democracy_Transnational_Societies.pdf.

CDD. 2022. Implementing the Voluntary Principles on Security and Human Rights in Cabo Delgado, Mozambique. [Online]. [Accessed 29 July 2024]. Available from: https://cddmoz.org/wp content/uploads/2022/08/Implementing-the-VPSHR-in-Cabo-Delgado-Mozambique_ENG.pdf.

CIP. 2010. Sobre o Registo de Cartões SIM Diploma Ministerial incoerente, ilegal e anticonstitucional. Observatório de Direito nº 1, CIP, 2010. [Online]. [Accessed 05 December 2020]. Available from: https://macua.blogs.com/files/observatório-de-direito-nº-1.-registo-de-cartões-sim-é-ilegal-e-anti-constitucional.-documento-do-cip-2010.pdf.

CIP. 2023. Uncovering the Costs of the War in Cabo Delgado: A Comprehensive Analysis of Fiscal Impacts and Multidimensional Challenges. [Online]. [Accessed 29 July 2024]. Available from: https://www.cipmoz.org/wp-content/uploads/2023/11/Uncovering-the-Costs-of-the-War-in-Cabo-Delgado.pdf.

Do Rosário, D. M. 2014. Eleições e corrupção em Moçambique. In: Cunha, I. and Serrano, E. eds. *Cobertura jornalística da corrupção política. Sistemas políticos, sistemas mediáticos, enquadramentos legais*. Lisboa: Aletheia Editores, pp. 124–48.

Do Rosário, D. and Guambe, E. 2023. Decentralising fraud: new models of electoral manipulation during the 2019 general elections in Mozambique. *Journal of Southern African Studies*, 49(4), pp. 677–95.

[Online]. Available from: https://doi.org/10.1080/03057070.2023.2291897.

FES and MISA. 2018. African Media Barometer – Mozambique 2018. Windhoek: FES. [Online]. [Accessed 29 July 2024].

Forquilha, S. and Orre, A. "Transformações sem mudança? Os conselhos locais e o desafio da institucionalização democrartica em Moçambique". In DE BRITO, L. et al. [(Org.) 2011]. Desafios para Moçambique 2011. Maputo: IESE, pp. 35–53.

Forquilha, S. and Gonçalves, E. 2022. Critical Issues on Social Accountability in Mozambique. *IESE*. [Online]. [Accessed 29 July 2024]. Available from: https://www.iese.ac.mz/wp-content/uploads/2022/10/CadernoIESE24E-SFEG.pdf.

Furtado, C. 1997/1998. Democracia em África: Possibilidades e limites. *África – Revista do Centro de Estudos Africanos/USP*. 20(1), pp. 199–217.

Georgiev, V. 2022. Oversight of security and intelligence services in republic of Bulgaria. *Politics & Security*. 6(2). doi:10.5281/zenodo.6823971

Gilbert, L. and Hohseni, P. 2011. Beyond authoritarianism: The conceptualizations of Hybrid Regimes. *Studies in Comparative International Development*. 46, pp. 270–97.

Hanlon, J., 2021. Collapsing electoral integrity in Mozambique. *Journal of African Elections*, 20(1), pp.44–66. https://www.eisa.org/storage/2023/05/2021-journal-of-african-elections-v20n1-collapsing-electoral-integrity-mozambique-eisa.pdf.

INCM. 2017. Registo de cartões "SIM" garante ao publico segurança e serviços de valor acrescentado. In: *25 anos do INCM – Instituto Nacional das Comunicações de Moçambique*, pp. 7–10. [Online]. [Accessed 21 January 2012]. Available from: https://www.arecom.gov.mz/index.php/sala-de-imprensa/telecomunicar/154-suplemento-25-anos-do-incm-edicao-especial-1/file.

Levitsky, S. and Way, L. A. Elections without democracy: The rise of competitive authoritarianism. *Journal of Democracy*. 13(2), pp. 51–65.

Macamo, E. 2014. Cultura política e cidadania em Moçambique: Uma relação conflituosa. In: De Brito et al. *Desafios para Moçambique 2014*. Maputo: EISE, pp. 41–60.

Machava, B.L. 2011. State discourse on internal security and the politics of punishment in post-independence Mozambique (1975–1983). *Journal of Southern African Studies*. 37(3), pp. 593–609.

MISA. 2024. Processo de legislação sobre Direitos Digitais, em Moçambique, deve garantir a protecção de dados, a privacidade e reduzir riscos de vigilância digital. Policy Brief. [Online]. [Accessed 29 July 2024]. Available from: https://www.misa.org.mz/index.php/quem-somos/planos-e-relatorios/legislacao/155-policy-brief-legilacao-sobre-direitos-digitais-mocambique.

MISA-Moçambique. 2020. Estagio da liberdade de imprensa em 2019: Apagão de informação e as perseguições contra a imprensa em Cabo-Delgado. *MISA*. [Online]. [Accessed 29 July 2024]. Available from: https://www.misa.org.mz/index.php/publicacoes/relatorios/relatorio-2008/98-estagio-da-liberdade-de-imprensa-em-mocambique-2019-apagao-de-informacao-e-as-perseguicoes-contra-a-imprensa-em-cabo-delgado/file.

MISA-Moçambique. 2021. Relatório sobre o estado da liberdade de imprensa e de expressão em Moçambique (2019–20). Maputo: MISA-Moçambique. *MISA*. [Online]. [Accessed 29 July 2024].

MISA-Moçambique. 2023. Liberdades de imprensa e direitos humanos em Moçambique: das violações contra jornalistas à vulnerabilidade dos cidadãos no ambiente online. *MISA*. [Online]. [Accessed 29 July 2024]. Available from: https://www.misa.org.mz/index.php/publicacoes/relatorios/relatorio-2008/143-relatorio-sobre-a-liberdade-de-imprensa-e-dh-em-mocambique-2022/file.

Ngoenha, S, Do Amaral, G. and Nhumaio, A. (2020). "Cabo Delgado e o risco sistémico da guerra em Moçambique", in Forquilha, S. Org. (2020). Desafios para Mocambique 2020. IESE. Maputo, pp 35–46.

Nhanale, E. 2019. A Cobertura dos Media sobre a Corrupção em Moçambique: Um 'contra-poder' Abalado? Maputo: CEC.

Nhanale, E. 2021. Electronic surveillance in Mozambique: The risks and suspicions in a context of authoritarianism and military conflict. [Online]. [Accessed 29 July 2024]. Available from: http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/report_04_2021_electronic_surveillance_mozambique_masterset.pdf.

Nhanale, E. 2024. Registo biométrico de cartões SIM: Que riscos para a proteccao de dados dos cidadãos e vigilância indevida? *Jornal Magazine Independente*, 20 de Feverireo de 2024, pp. 12–13.

Nhanale, E. and Cossa, M. 2024. As questões críticas e os fatores que condicionam as liberdades de imprensa em Moçambique. *Animus, Revista Interamericana de Comunicação Midiática*. 22(50), pp. 83–105.

Pereira, J.C.G. and Nhanale, E. 2014. *As eleições geraias de 2014 em Moçambique: Análise de questões fundamentais*. Joanesburgo: OSISA.

Raab, C.D. 2017. Security, Privacy and Oversight. In: Neal, A. W. ed. *Security* *in a Small Nation Scotland, Democracy, Politics*. Cambridge: Open Book Publishers, pp . 77–102.

Shenga, C. and Mattes, R. 2009. Cidadania acrítica numa sociedade de baixa informação: os moçambicanos numa perspectiva comparativa. In: De Brito, L. et al. *Cidadania e Governação em Moçambique. Comunicações Apresentadas na Conferência Inaugural do Instituto de Estudos Sociais e Económicos*. Maputo: IESE, pp. 119–69.

Sirrs, O. 2021. Soviet Bloc Security Services and the Birth of New Intelligence Communities in Mozambique and Angola. In: Shaffer, R. ed. *African Intelligence Services: Early Postcolonial and Contemporary Challenges*. London: Rowman & Littlefield, pp. 69–90.

Snowden, E. 2019. *Vigilância massiva: Registo permanente*. Traducao Mário Dias Correia. Lisboa: Planeta.

Tsandzana, D. 2016. Mozambican government is spying on its citizens according to @Verdade. *Global Voices*. [Online]. [Accessed 29 July 2024]. Available from: https://advox.globalvoices.org/2016/05/16/the-government-of-mozambique-is-spying-on-its-citizens-according-to-verdade/.

Zeca, E.J. 2021. Serviçoes de Inteligência em Moçambique: Instituições, Dinâmicas e Operações. Maputo: Academia de Altos Estudos Estratégicos.

Legislation

Decree No. 13/2023. Approves the Regulation of the Registration of Telecommunications Services Subscribers and Repeals Decree No. 18/2015, of 28 August. Official Gazette, I SERIES – Number 69. Tuesday, 11 April 2023.

Diploma Ministerial n° 153/2010, Boletim da República, I Série, no 37, 15/09/2010.

State Secrecy Law– Law No. 12/79 of 12 December. Maputo: National Press.

Regulation of Law No. 12/2012, of 8 February, which Revises Law No. 20/91, of 23 August, which Establishes the State Information and Security Service (SISE).

Popular Republic of Mozambique, 'Law of Crimes against the Security of People and the Popular State', Tempo, March 4, 1979.

Amnesty International, Reports on the Practice of Torture in the Popular Republic of Mozambique (Maputo: Amnesty International, 1985).

Constitution of the Republic of Mozambique (1990). Maputo: National Press.

Public Probity Law – Law No. 16/12 of 14 August. Maputo: National Press.

Law of Associations – Law No. 08/91 of 18 June. Maputo: National Press.

Law to Combat Corruption. Law No. 6/2004, of 17 June. Maputo: National Press.

Law of Crimes Against State Security – Law No. 19/91 of 16 August. Maputo: National Press.

Press Law – Law No. 18/91 of 10 August. Maputo: National Press.

Right to Information Law – Law No. 34/14 of 31 December. Maputo: National Press.

Political Parties Law – Law No. 07/91 of 23 January. Maputo: National Press.

Freedom of Assembly and Demonstration Law – Law No. 9/91 of 18 June. Maputo: National Press.

State Secrecy Law – Law No. 12/79 of 12 December. Maputo: National Press.

CHAPTER SEVEN

The democratic subsidy in Namibia's intelligence oversight mechanisms

Frederico Links and Phillip Santos

Introduction

The ideal framework for organising society at all levels is generally accepted to be that of a democracy. Nonetheless, the very notion and practice of democracy is often highly contested and even questioned by some whose own societies embrace or impose, at best, limiting and highly centralised systems of governance and, at worst, outrightly authoritarian and repressive governance systems. In this chapter, we use an agonistic normative idea of a democracy to evaluate the place and implications of intelligence services to limiting or enhancing democratic governance in Africa and Namibia in particular. We acknowledge that there is no single understanding of, or consensus on, what a democracy is, but also underscore the axiom that there are certain fundamental elements that are consistently associated with democratic systems. These include, among others, guarantees for and protections of fundamental human rights, open, participatory and inclusive governance systems and the rule of law (see Held, 2006; Christians et al., 2009). This does not mean that democratic societies are or should be impervious to social contestations as this is far from the truth. We draw on Mouffe (1999; 2005) and Gramsci's (1957/2021) work, to argue that conflict is indeed an immanent element of democratic politics and polities. Nonetheless, it is useful to be specific about the kind of conflict that is consonant with democratic politics. In our view, social conflict over everyday governance issues which simmers below the plane of violence and reflects contestations over exigent social issues in society is, arguably, not only immanent in a democracy, but also desirable, as it is hardly the case that consensus and homogeneity in public opinion will ever be achieved, let alone crystallise (see Mouffe, 1999; 2005). As such, the question about how to properly provide oversight of the operations of intelligence services in any society is likely to arise, mutate and stabilise in the flux and flows of everyday discourses in formal political institutions and processes, as well as in the public domain. Contestations over how best to integrate the operations of intelligence services within the architecture of a democratic society and its institutions will ineluctably be shaped by the politics of which they are a part within a competitive multiparty and multi-stakeholder democracy.

In this chapter, we argue that debates and contestations about the role and limits of intelligence services, to the extent that they are occasioned and manifested, are not an aberration of democratic politics, but constitute the sinews of its imperfect fabric. These debates reflect the range of views about how best to organise and govern society at particular points in its history. Such debates are mostly possible and nourished in democratic rather than authoritarian societies. It is in this context that we analyse debates over the accountability of intelligence services in Namibia. As some have already highlighted, debates about the role of intelligence services in Namibia reflect the tension between the legacy of the liberation struggle and contemporary preoccupation with the virtues of democratic politics, which put citizens' rights at the centre of the operation of public institutions and delivery of public services (Bolliger, 2023). We, therefore, examine the dimensions of this dialectic and locate it within radical conceptions of democratic politics. The chapter starts off by outlining the historical and contemporary context within which to understand the organisation and practices of intelligence services in Namibia. Its theoretical and philosophical framing of democracy is discussed in the next section, after which the chapter explicates the existing paradox of Namibia's democracy in so far as this pertains to the role of intelligence services in the country. An attempt at imagining a democratic framework for the operation of intelligence services in Namibia is presented just before concluding the chapter. Originally, this chapter was meant to be based on qualitative interview data gathered from a range of key informants, including former and current intelligence service officials, civil society and journalists, among others. However, the authors could not gather the necessary data, owing to challenges in securing ethics clearance for the study, hence this analytical chapter.

Historical and contemporary context

Postcolonial Namibia has significantly upended the brutally oppressive, genocidal, authoritarian, sectarian and racist socio-economic and political system of its former colonial oppressors, Germany and apartheid South Africa. Not only is Namibia acknowledged and highly regarded as a multiparty constitutional democracy, it has also significantly created opportunities for its previously marginalised and brutalised Black population (see Global State of Democracy Initiative, 2024). For example, according to the World Bank, Namibia 'halved the poverty rate between 1993 and 2016' (2021, p. 1). However, despite these achievements and its status as an upper-middle-income country, Namibia continues to grapple with social challenges such as inequality (with the second-worst margin in the world), poverty and unemployment (World Bank, 2021). In addition, the country's democratic system is still a work in progress, a reality evident regarding the shaky transparency and accountability of its security sector, in particular, the intelligence service, which is the focus of this chapter.

When the South-West Africa People's Organisation (SWAPO) party turned up at the newly instituted Constituent Assembly, following the landmark elections of November 1989 that saw Namibia gain independence from then apartheid South Africa, it did not have a democracy-inclined constitutional proposal to place on the negotiating table, and certainly not anything that contained a strong bill of rights (Wiechers, 2010). What it did have were Soviet-style proposals for the organisation and structure of the future

Namibian state, heavily drawing on 'East European ideology and constitutional thinking' (Wiechers, 2010, p. 87) that emphasised strong party control over all arms of state power, the executive, legislature and judiciary. The SWAPO proposals which, according to Wiechers (2010), were officially never unveiled at the post-election constitutional negotiations, in the wake of the collapse of the East European communist bloc following the fall of the Berlin Wall in 1989, had become 'extremely suspect' and the party rightly surmised that its proposals were out of step with the historical moment. In the end, as the constitutional negotiations were about to get under way, Wiechers (2010) recounts, SWAPO hastily cobbled together a 'new' position that resembled the 1982 Constitutional Principles,[1] a move that ultimately enabled the relatively smooth crafting and drafting of a constitution in two months, as the majority of the proposals tabled by other parties for inclusion in the future Constitution were in some way also based on these same principles. However, while the 1982 Constitutional Principles reflected broad democratic convictions and the Namibian Constitution that came into force on 21 March 1990 was substantially democratic, the ruling party's attitude to governance in the post-independence period continued to reflect the undemocratic, old East European ideology and thinking with which it had arrived at the negotiating table in late November 1989.

We highlight this point to argue that since its birth in April 1960, through the liberation struggle years (from 1966 up to 1989), and up to independence on 21 March 1990, SWAPO had not been and was not a perfect movement for democracy. While the party started out, in its very first political manifesto in 1961, by espousing democracy and freedom, by the mid-1970s, as Du Pisani and Lindeke (2009,

[1] The 1982 Constitutional Principles actually emerged from an all-party conference convened in Geneva, Switzerland in early 1981, under the supervision of the Western contact group (USA, UK, France, Canada and West Germany) to flesh out matters related to the Constituent Assembly and the content of the future Namibian Constitution. In 1982 these principles became part of UN Security Council Resolution 435 of 1978, which prescribed the processes and conditions for Namibian independence from apartheid South Africa.

p. 6) note, it had started 'breathing the air of socialism'. By then it had become the pre-eminent pro-independence movement and the radical change sought in its political programme reflected a centralising of power in the hands of a coterie of senior leaders, who in post-independence Namibia are colloquially referred to as the 'old guard' (Dauth, 1996). Saunders (2003, p. 88) notes that by independence SWAPO had been 'highly authoritarian in its practices' and hierarchical. By then (the late 1980s) as Melber (2003, p. 14) points out, it was 'not democratisation that was the priority agenda item for Namibia, but decolonisation'. As Melber (2003, p. 14) states:

> The agenda was first and foremost shaped by the goal to establish a formally legitimate and internationally recognised sovereign Namibian state. By implication, many of the forces involved may have had the expectation that this required democracy as the basis of a lasting political system. Explicit evidence for this, however, remains scarce and scattered.

Like many liberation movements the world over, SWAPO had over the course of the war for independence increasingly organised itself (both in response to perceived infiltration by the enemy and in efforts to ward off internal rebellions and leadership discontents over the years) along 'strictly hierarchical and authoritarian lines, otherwise they would hardly have had any prospect of success' (Melber, 2003, p. 12). That is to say, the culture within the party and the movement was not one that could be said to have been democratic in nature. This means that while SWAPO's liberation fighters were fighting the brutal authoritarianism of apartheid colonialism, they were themselves prone to authoritarian violence and coercion from within.

In this regard, Saul and Leys (2003, p. 70) are adamant that there 'is no room for doubt as to the seriousness of the indictment levelled against the SWAPO leadership regarding its human rights abuses in exile. There is a wide range of recorded testimony.'. They, and others, have pointed to the organisation's pre-independence security and intelligence apparatus, firmly in the grip of the movement's senior leadership, which with time had become increasingly paranoid and authoritarian in response to real and perceived internal and external threats. The organisation's security apparatus was primarily responsible for the perpetration of widespread human-rights abuses among its rank-and-file members, especially from the late 1970s and throughout the 1980s, up until the independence elections in November 1989. Links (2019, p. 5) notes that in

> the process of ostensibly countering enemy espionage and infiltration – in a prolonged campaign that reportedly involved arbitrary arrests and detentions, torture, mutilation, and mass disappearances – the organisation had itself built a formidable internal security and intelligence capability and apparatus. Historical and witness accounts paint a picture of a Soviet-style 'secret police' that wielded power with ruthlessness and impunity.

In other words, the SWAPO leadership relied heavily on this Soviet-style 'secret police' to maintain command and control through repression, coercion and a culture of fear among the movement's rank and file (Saul and Leys (2003, p. 70). This centralised command over internal security and intelligence functions at the very top of the movement was ultimately carried over into independent Namibia, as we shall discuss later in this chapter.

What the foregoing illustrates is that at the time of Namibia's attainment of independence on 21 March 1990, the political force that was to dominate politics in post-independence Namibia, SWAPO, following the November 1994 presidential and parliamentary elections, was not imbued with strong democratic convictions as noted by Dobell (1998). What this meant, practically, regarding the transfer of state power post-independence was that an authoritarian system of government was taken over by a partly authoritarian-inclined new political elite through a process in which 'new societies carried within them essential elements of the old system which they had fought' (Melber, 2003, p. 12). So, even though the transfer of political and state power came about through democratic means, the governance structures of the 'old' state and the culture of the newly installed governing elite were not democratically inclined (Wiechers, 2010).

Arguably thus, the 'new' post-independence state to some extent initially and significantly appropriated and reflected undemocratic governance tendencies and approaches of the old apartheid state. This tendency was not unique to the Namibian context, of course, but was evident in other postcolonial, postindependence societies on the continent as well.

Regarding intelligence governance, Du Pisani (2003, p. 2) notes that the state and the security sector, which includes the intelligence services, are 'intimately connected' and that the nature of the security sector reflects the nature of the state, and vice versa. In the Namibian context, this has historically meant that the intelligence, and broader security services have largely been shielded from any sort of meaningful public scrutiny. This lack of transparency is a core characteristic of the postindependence Namibian state and is, as already noted, a hangover of the Cold War era ideological disposition of the SWAPO ruling elite, which has allowed the establishment, as Bolliger (2023) argues, of an authoritarian intelligence culture in a democratic state. On a practical level, this has meant that post-independence intelligence-related policy and governance matters have not tended to be publicly discussed and debated (Du Pisani, 2003). By effectively casting the secrecy shroud of 'national security' over any and all things intelligence-related, Namibian authorities have to a large extent succeeded in silencing any debate over or criticism of its intelligence activities and governance practices, thereby ensuring that such matters are not accorded appropriate importance or, for that matter, widely understood within the broader polity. In this way, the Namibian ruling elite has for more than three decades managed to avoid transforming intelligence governance to reflect a significantly more democratic dispensation. As Du Pisani (2003) notes, regarding democratic governance of the broader state security sector, this should be read and derived from subarticle 1.2 of the Namibian Constitution, 'which recognises the sovereignty of the people as the foundation for state power'. Du Pisani concludes that the state of democratic governance – marked by significant deficiencies and shortfalls – of the broader security sector, and notably the intelligence service, signifies that Namibia is still in a state of democratic transition and consolidation. At the time of writing this chapter, Du Pisani's assessment was already just over two decades old, and the situation – deficiencies and shortfalls in democratic governance of the state security sector – remains true, as demonstrated by Bolliger (2023) and others.

Agonistic pluralism qua democratic politics

The operations of intelligence services are counterintuitive to democratic sensibilities for various reasons, prominent among which is the element of openness that juxtaposes against the former's penchant for secrecy. By their very nature, democratic societies are open and democratic institutions accountable to citizens, and yet intelligence services are usually neither open nor accountable due to their secretive nature (see Hillebrand, 2012). It has also been generally acknowledged that intelligence services are imperative for security reasons and for generating relevant intelligence for various sectors of a country's sociopolitical and economic landscape to help inform policymaking (see Caparini, 2007; Hillebrand, 2012). Nonetheless, given the potential risk of abuse and excess in the operations of intelligence services, it is imperative that some effective oversight be provided on this sector of governance (Caparini, 2007; Hillebrand, 2012; Aradau and McCluskey, 2022; Kniep et al., 2024). Without this oversight, it is very easy for intelligence services to be abused in ways that egregiously violate human rights, reminiscent of operations of such notorious organisations as the Gestapo in Hitlerite Germany (Stackhouse, 2021), the NKVD and later KGB in the Soviet Union (Bateman, 2016), the United States' Central Intelligence Agency (Absher et al., 2023), the Stasi of East Germany (Lichter et al., 2021) and almost all intelligence services of colonial governments on the African continent and post-independence authoritarian systems (see Shaffer, 2021).

As some have argued, the boundaries of oversight mechanisms are as amorphous as they are diverse (see Kniep et al., 2024). Broadly speaking, they can be categorised in terms of the binary between formal and informal arrangements, a point to which we shall return below. However, they can also be broken down into more specific mechanisms that include, inter alia, executive-level oversight, legislative oversight, judicial oversight, international oversight, oversight by the media, civil society and political-interest groups, among others (Caparini, 2007; Hillebrand, 2012; Kniep et al., 2024). Considering the complex and overdetermined oversight matrix evident in most democracies, we argue that the ideal typical normative framework for thinking oversight of intelligence services is Mouffe's (1999; 2005) approach to radical democracy via the model of agonistic pluralism. The approach takes, as its departure point, the view that not only is conflict a necessary element of democratic societies, but it is also inherent and ineradicable (Mouffe, 1999; 2005). As such, contestations and differences about what role the country's intelligence services should play reflect actual debates about what kind of society Namibians want. Such debates are ineluctably informed by the country's sociohistorical memories, citizens' lived experiences in contemporary Namibia and citizens' aspirations for a democratic Namibian imaginary, going into the future. These are higher-order considerations whose nature and shape can be discerned from a refraction of perceptions about the organisation and operation of the country's intelligence services.

According to Mouffe, consensus over such big social questions is hardly achievable and, when it is achieved, such consensus remains tenuous, given the immanence and ineradicable nature of social conflict in democratic societies (1999; 2005). As the social world itself transforms, new challenges and questions about the role of public institutions, not least intelligence services, will emerge and be the subject of further debates about engagement with and reformulation of oversight mechanisms. The social implications of such factors as artificial intelligence, climate change, inequality, geopolitical tensions, transterritorial threats posed by terrorism, and the displacement of people and war, among other things, require dynamic and versatile intelligence services, albeit operating within democratic parameters. It is this latter proviso which casts conflict as ineradicable and the transformation of intelligence services as an existential imperative. For example, threats such as those posed by terrorism, artificial intelligence and geopolitical tensions may require some significant degree of secrecy and flexibility which may undermine effective formal and informal oversight of the operations of intelligence services.

The contested nature of democratic space can also be aptly explicated in terms of Gramsci's conception of hegemony. For Gramsci, hegemony is achieved through moral leadership and the subsequent consent of dominated social groups (1957/2021). However, it has also been argued that every hegemonic instance is always in a precarious and unstable position that has to be struggled for in perpetuity as it is in uneasy co-existence with counterhegemonic forces which challenge the very instance of such hegemony (Miliband, 1990). In democratic societies, this is manifested in the continuous contestations between different social and interest groups over how best to organise society for the maximum benefit of all. This terrain of political contestation is marked by competing interests and interpretations of the social sphere, which interpretations are reflected in policymaking, the formulation of national laws, development policies, the balance between fundamental freedoms and their limitation, governance structures and the structure and condition of formal and informal oversight mechanisms, inter alia. It is on this basis that we argue oversight mechanisms on intelligence functionaries in Namibia must be analysed in a holistic manner. For example, it is our contention that informal mechanisms of oversight are as important as formal ones, and they operate both in contest and to complement each other. Either way, this can enhance oversight of, and the accountability of, intelligence functionaries. First, where they complement each other, the whole oversight edifice becomes that much stronger and, where they are in tension, the issues at stake are made visible for further debate, consideration, negotiation and resolution. That way, democracy is occasioned in contested praxis. Second, contestations about the role of intelligence services in and of themselves are symptomatic of functional macro-oversight mechanisms and democratic agonism. In the absence of democracy, it is almost unheard of that the operations of intelligence functionaries would even be a subject of scrutiny and contestation.

Furthermore, as some have observed, formal oversight mechanisms tend to be either too close to and dependent on the very institutions over which they are expected to provide oversight, or they may be reverent of and play an advocacy role for intelligence functionaries, which stunts their oversight potential (Kniep et al., 2024; Caparini, 2007). As such, more open and democratic societies, such as Namibia, enable multilayered and diverse points of oversight of intelligence services, even though formal mechanisms of oversight are either absent or under-developed, and operate in collaboration with the state and its intelligence infrastructure. In the following section, we draw on empirical material to demonstrate that, although Namibia's formal oversight mechanisms on intelligence functionaries require more work, the country's democratic subsidy affords and expands the scope of such oversight mechanisms beyond the limits of formal arrangements and realities.

Tension between democratic and authoritarian tendencies in Namibia

The bane of post-independence politics in Africa has been the tension between continuities of authoritarian colonial legal/institutional arrangements and discontinuities necessitated by the constitution of democratic post-independence polities. This tension is reflected in the schizophrenic co-existence of repressive legal provisions inherited from the colonial state and the progressive constitution of a postindependence democratic dispensation, as evinced, primarily, in democratic national constitutions. For example, as shown by Fesmedia Africa's African Media Barometer country reports, a significant number of African countries have retained the colonial Official Secrets Laws in one form or the other. Almost invariably, most postindependence African states retained the colonial security infrastructure that bears the authoritarian tinge of its original architects (Shaffer, 2021). Given the incompatibility between these and the imagination and subsequent constitution of postindependence democratic African societies, the place and role of intelligence services inevitably becomes a contentious and urgent issue. As such, colonial traces in the constitution and governance of post-independence intelligence systems, of necessity, require that there be effective formal oversight mechanisms and a broader enabling democratic environment where informal oversight structures and functionaries can emerge and operate unencumbered.

As some have noted, formal oversight mechanisms can be institutionalised nationally and internationally, through inter alia, relevant legislation and judicial mechanisms, parliamentary and special investigative bodies, as well as intelligence functionaries' own internal oversight mechanisms among others (see Goldman and Rascoff, 2016; Gill, 2020). However, beyond these are also informal oversight structures which include, among others, news media through their monitorial role (Christians et al., 2009; Hillebrand, 2012), as well as civic society and whistleblowers, among others (Kniep et al., 2024). Be that as it may, the latter's efficacy is contingent on an enabling democratic environment. Free, plural, independent and diverse news media with unfettered access to information; a vibrant, free and independent civil society; along with protected whistleblowing channels are indispensable pre-conditions for effective informal oversight mechanisms. In this section, we argue that despite gaps in Namibia's formal intelligence oversight mechanisms, the country's democratic subsidy has so far enabled some functional informal intelligence oversight activities. This does not mean nor suggest the redundancy of formal oversight mechanisms. Rather, we believe in the need for and primacy of formal intelligence oversight systems because they are required to be accountable to the citizenry, but we also acknowledge, in some cases, both the fact of their ineffectiveness, at best, and their absence, at worst, which necessitates functional informal intelligence oversight. In the ensuing discussion, we explicate the state of both formal and informal oversight mechanisms, showing how the country's democratic subsidy has allowed some scrutiny over intelligence services in the absence of effective oversight structures and functionaries.

Gaps in Namibia's intelligence oversight

As has already been discussed and as various authors (Saul and Leys, (2003; p. 70) Links, 2019; Bolliger, 2023) have noted, the authoritarian intelligence culture that permeated SWAPO's internal security apparatus during, especially, the latter half (mid-1970s to 1989) of the liberation-struggle era has been carried over into the postindependence transitional democratic dispensation. This authoritarian intelligence culture has been built into Namibia's legal framework that has been established to govern the operational and intelligence-gathering activities of the Namibia Central Intelligence Service (NCIS), the formal successor in independent Namibia to SWAPO's security and intelligence arm of the liberation-war era. This obtains insofar as such laws significantly limit any sort of meaningful formal democratic oversight of the operations and, specifically, the communications surveillance function of the NCIS's intelligence-gathering activities.

Du Pisani (2003, p. 3) posits that governance means more than 'government' and 'implies a productive partnership between the legislature, the executive, the civil service, civil society and the academy' in handling intelligence-related matters. Interestingly, he does not mention the media as part of this 'productive partnership'. That said, here it is necessary to note that oversight structures in 'the legislature, the executive, the civil service' would constitute the formal intelligence governance structures or mechanisms, while 'civil society and the academy' (along with the media) would constitute the informal. Du Pisani (2003), drawing on Weiss and Gordenker (1996, p. 42), loosely takes governance to refer to 'intergovernmental relations, norm and policy setting, policy execution, political/public oversight at both the national and multilateral (sub-national) levels'. In the Namibian context, intelligence governance should be discussed in the context of a liberal democracy, since the Constitution of the Republic of Namibia establishes Namibia as a liberal democracy. Ideally, Du Pisani notes, in a liberal democracy, intelligence governance should take the form of a 'democratic political control' dispensation, which he describes as follows:

> Democratic control implies that the [intelligence service] acts in ways which the citizens as a whole approve of. This in turn means that the government which the people elect is the first source of control, followed by parliament, followed possibly by

> the courts (to ensure the integrity of the constitution). The issue goes beyond that of narrow control, and means a complex interrelationship between the state, political society and civil society (2003, p. 4).

Furthermore, Du Pisani (2003, p. 4) argues that the 'key principles of good governance in the security sector', as espoused by the United Kingdom (UK) government's former Department for International Development (DFID),[2] best exemplify the 'democratic political control' of intelligence services in liberal democracies. These principles can be summarised as follows:

- Security sector organisations, particularly the security forces, are accountable both to elected civil authorities and to civil society.
- Security sector organisations operate in accordance with international law and domestic constitutional law.
- Information about security sector planning and budgeting is widely available, both within government and to the public, and a comprehensive and disciplined approach to the management of defence resources is adopted.
- Civil-military relations are based on a well-articulated hierarchy of authority between civil authorities and the defence forces, on the mutual rights and obligations of civil authorities and the defence forces, and on a relationship with civil society that is based on the respect for human rights.
- Civil authorities have the capacity to exercise political control over the operations and expenditure of the security forces and civil society has the capacity to monitor the security forces and provide constructive input to the political debate.
- An environment exists in which civil society can actively monitor the security sector and be consulted on a regular

[2] The Department for International Development was dissolved in September 2020 and has been superseded by the Foreign, Commonwealth and Development Office (FCDO).

basis on security policies, resource allocation and other relevant issues.
- Security-force personnel are adequately trained to discharge their duties in a professional manner consistent with the requirements of democratic societies.
- Fostering an environment supportive of regional and subregional peace and security has a high priority for policy makers (DFID, 2000).

It is against this conceptual backdrop of intelligence governance that the following discussion of the tensions between democratic and authoritarian tendencies proceeds.

Operational governance oversight

The operations and activities of the NCIS are governed by the Namibia Central Intelligence Service Act (Act 10 of 1997), which details the powers, duties, functions and general mandate of the NCIS, as well as specifying oversight entities. The NCIS Act repealed the old South African National Intelligence Act (Act 19 of 1987). Regarding intelligence oversight, the law makes it clear that the Director General of the NCIS reports directly to the State President, a scenario that Du Pisani (2003, p. 2) argues is consistent across Southern Africa as a legacy and consequence of the 'ideological context of the Cold War, the protracted armed struggle against apartheid, the material interests that underpin the security sector and the state and the character of governance'. He notes that 'Security continues to be the preserve of the Head of State or a select few in the executive arm of government, especially since the survival of state elites is often the greatest security concern' (Du Pisani, 2003, p. 3).

That said, the law also makes provision for some limited oversight of the operations and activities of the NCIS by the Namibian National Assembly's Standing Committee on Foreign Affairs, Defence and Security. Nevertheless, this oversight provision can still be circumvented under certain conditions at the discretion of the Director

General of the NCIS or the State President, or both. Notably, despite the fact that the Namibian state was founded on the principle of the separation of powers, with the legislative and judicial branches, theoretically and practically, expected to serve as effective checks on the executive branch, the Namibian Parliament, a bicameral parliament consisting of the National Assembly and the National Council, has never, in the 34 years of its existence, served as a robust check on the executive branch (Lindeke, 2007). There are both political and structural reasons for this. Politically, given its dominance of the legislature since independence, SWAPO has effectively controlled the legislative agenda. Similarly, for most of the history of the Namibian parliament, the executive has numerically dominated the benches, with ministers and deputy ministers outnumbering backbenchers and opposition parliamentarians for most of the last three decades (Tjirera and Hopwood, 2009). As such, Lindeke (2007, p. 8) argues that 'party discipline and cabinet dominance have created a monopoly of the executive branch over law-making'. He adds, citing Melber (2006), that the 'National Assembly lacks robust debates on policy for the most part and is widely considered a rubber stamp for the Executive which has dominant numbers' (Lindeke, 2007, p. 11). Structural deficiencies – budget, staffing, policy and research capacity and so on – have contributed to and exacerbated the dysfunctions of the Namibian legislature (Links et al., 2023).

A major casualty of the dysfunctions of the Namibian legislature over the past decades has been the parliamentary committee system, which has never functioned optimally (see Lindeke, 2007; Tjirera and Hopwood, 2009; Links et al., 2023). Transforming the parliamentary committee system to enable the Namibian parliament to play its oversight role more effectively formed a core part of the National Assembly's *Agenda for Change* (1995). However, the *Agenda* never really got off the ground over the nearly two-and-a-half decades since its declaration (Lindeke, 2007; Links et al., 2023). It is only over the last few years, since 2021 that there appears to have once again been significant discussions and steps taken to revive the *Agenda*. What the foregoing illustrates is that the Namibian legislature, and specifically, and especially, the parliamentary committee system, has to date not been an effective oversight mechanism or check on the Executive branch in any sector. This effectively means that, as Lindeke (2007, p. 3) argues, from the beginning Namibia has had a 'strong or executive presidential system' with a cabinet, which has traditionally meant that 'negotiations and decisions occur within Cabinet and between ministries out of public and parliamentary view' (Lindeke, 2007, p. 8).

Against this backdrop, the notion that the Namibian National Assembly's Standing Committee on Foreign Affairs, Defence and Security is an effective oversight mechanism over the operations and affairs of the NCIS seems a rather quaint pretence. To underscore this point, in mid-2018 it was reported that in all the years of its existence up until then, 'the spy agency has apparently never submitted a report or made an appearance before' the National Assembly's Standing Committee on Foreign Affairs, Defence and Security (Links, 2019, p. 6). Media reporting at the time further stated that the committee did 'not have access to any operational information of the agency and as such has not submitted a report to parliament' (Links, 2019, p. 6). To emphasise this point further, it is imperative to consider that the NCIS has argued in court, in a high-profile 2018 High Court case brought against a newspaper to attempt to muzzle it, using the apartheid-era Protection of Information Act (Act 84 of 1982), from reporting on operational and financial matters that had the appearance of corruption, that, given what it considered the supremacy of its national security mandate, it should not be subject to either parliamentary or judicial oversight.[3] Ultimately, the court ruled against the NCIS's media-muzzling attempt, in a judgment that was upheld on appeal by the Namibian Supreme Court in 2019, and reaffirmed that in a liberal democracy all state entities, including those in the state security sector, were subject to the rule of law and judicial oversight.

Additionally, in the same year, two other matters that reflected an absence of meaningful official oversight of the NCIS's affairs,

[3] The case was *Director General of the Namibia Central Intelligence Service and Another v Haufiku and Others* (107 of 2018) [2018] NAHCMD 174 (18 June 2018), and the judgment can be read *here*.

explosively came into public awareness. The first was when in March 2018 it was revealed that the NCIS had been paying for the running of the offices of two Directors-General since 2015 because the old Director General, Lucas Hangula, had refused to vacate his office and retire when the new Director General, Philemon Malima was appointed in early 2015. Secondly, it also emerged that a senior NCIS official, reportedly responsible for crime intelligence, was found to have been stealing from and defrauding the service for nearly two decades to the tune of tens of millions of Namibian dollars. The matter was closed without going to trial when the official committed suicide in late 2018. These incidents taken together led Links (2019, p. 8) to conclude that:

> . . . the intelligence service seems to be riven with corruption, mismanagement and the waste of state resources, and has abused the mantras of secrecy and 'national security' to cover up (or attempt to) illegal activities within its ranks and structures. These sorts of practices have arguably created an internal culture founded on the belief that the NCIS was not answerable to the courts or parliament and can operate outside the law.

Surveillance governance oversight

Another key consideration is the nature of oversight in the context of communications surveillance governance. On paper, in terms of operational matters, the Namibian National Assembly's Standing Committee on Foreign Affairs, Defence and Security is mandated to provide a measure of formal public oversight over the communications surveillance activities of the NCIS. However, as has been noted earlier, with regard to operational matters, that the NCIS has also 'apparently never submitted a report or made an appearance before' the committee with regard to its intelligence gathering or surveillance activities (Links, 2019, p. 6).

The Namibian communications surveillance framework consists of the Namibia Central Intelligence Service Act (Act 10 of 1997) and the Communications Act (Act 8 of 2009). As indicated earlier, the

NCIS Act outlines the powers, duties, functions and general mandate of the NCIS, including the monitoring and interception of communications by its agents. The Communications Act, in Part 6 of Chapter V, also provides for the monitoring and interception of communications and is the primary communications surveillance-enabling law on the Namibian statute books. The framework, specifically in Section 24 of the NCIS Act, provides for some judicial oversight, by making it an offence for anyone to engage in communications surveillance without a warrant issued by a judge. Regulations issued under the Communications Act in April 2021 and April 2022, that brought into force Part 6 of the law on 1 April 2024, also provide for a warrant to be sought from either a judge or magistrate, in order to engage in communications surveillance.[4] Over the intervening years since 2009, when questioned about the status of regulations for Part 6, the standard response from the Ministry of Information and Communication Technology (MICT) had always been that consultations were ongoing (Links, 2019). That said, Part 6 of Chapter V of the Communications Act also provides for the setting-up of interception centres by the NCIS. The April 2021 regulations authorise mandatory SIM-card registration, while the April 2022 regulations provide for mandatory data retention and directs telecommunications and internet service providers to collect and store all communications data for a period of five years.

It should be noted that the new regulations also make provision for the Namibian Police Force to access customer information without court authorisation in urgent situations. These regulations were given further force in 2023 with the enactment of the Criminal Procedure Amendment Act (Act 7 of 2023), which in new sections, first, empower any police official to demand any information, document or data from anyone without a court order and, second, provide for any senior police official to gain access to the bank accounts and financial records of any person at any financial institution, once again without having to get a court order (Hubbard, 2024).

[4] These regulations can be viewed on the website of the Communications Regulatory Authority of Namibia (CRAN) at the following link: https://www.cran.na/sim-registration-awareness/.

That said, aside from the mandatory SIM-card registration and data-retention regime imposed on Namibians, a regime that effectively enables mass state surveillance – by being perpetually switched on to collect all the communications data of all telecommunications and internet users in Namibia, and storing such data for up to five years, irrespective of whether it is of investigatory interest or not – where the authoritarian intelligence culture also finds expression is in the gaps and challenges of the communications surveillance framework. The gaps and challenges that are the subject of the ensuing discussion were identified through a human-rights impact assessment of the communications surveillance framework conducted on behalf of the Windhoek, Namibia-based, Institute for Public Policy Research (IPPR) following the issuance of the regulations of April 2021 and April 2022 by Namibia's then Minister of Information and Communication Technology (ICT), Peya Mushelenga. The human-rights impact assessment was conducted by a South Africa-based, public-interest advisory firm, ALT Advisory, and a report was delivered to the IPPR in October 2022.[5] The ensuing discussion draws heavily from the report. The IPPR's human-rights impact assessment found that the communications surveillance framework 'falls short on a range of fronts' that would make for a more democratic oversight dispensation (IPPR, 2022, p. 28). These shortcomings are: lack of necessity and proportionality; lack of protections for metadata; provision for urgent warrantless access; lack of user notification; and a range of other transparency and oversight gaps. A brief unpacking of the issues raised by the assessment is warranted. That said, with regard to a lack of necessity and proportionality the study notes:

> Best practice dictates that the privacy violations inherent to communication surveillance demand that these powers be exercised only when necessary, when responding to the most severe crimes and threats to safety and security, and only where

[5] The report of this human-rights impact assessment remains unpublished, but in the possession of one of the authors of this chapter, namely Frederico Links, who had commissioned the study on behalf of the IPPR.

> less intrusive measures have failed. These elements are lacking or at best inconsistently applied in the Namibian framework (IPPR, 2022, p. 28).

In terms of a lack of protections for metadata, the study notes:

> The Namibian framework mistakenly assumes that communications data is less sensitive than the content of communications, and accordingly provides fewer protections and safeguards for its access. This is out of keeping with international best practice, which calls for all forms of communication data to be subject to the same rigorous protections and safeguards against access (IPPR, 2022, p. 29).

Concerning the provision for urgent warrantless access, it is found that, first, it is unusual to saddle a specific staff member, who might or might not be appropriately qualified to make such a decision, with the responsibility of whether to grant access to communications data in the possession of a given telecommunications service provider. Second, the assessment found that urgent warrantless access undermines the authority of the courts by allowing for accessing of sensitive data without judicial sanction. And, third, additional safeguards against abuse are absent, such as requiring law-enforcement or security agents having to seek authorisation from or provide formal notification of having accessed communications data after the fact to a relevant court (IPPR, 2022, p. 30). The study also points out that the Namibian interception framework lacks provisions for postinterception user notification.

On transparency and oversight gaps, the study notes that the framework does not provide for robust independent oversight, such as specialist judges or courts with expertise in the legal and technical questions around communications surveillance and human rights. In the same vein, the framework also does not provide for public reporting on communications surveillance-related activities. The study also found an absence of any robust complaints mechanism in the framework, such as an Ombud with powers to initiate investigations on public complaints regarding suspected surveillance abuse

(IPPR, 2022). As is demonstrated, the framework is devoid of critical transparency and accountability checks and balances that should ideally be in place in a liberal democracy. It is because of these significant weaknesses that the IPPR concludes 'a full reform process is recommended to provide better protections and safeguards for communications and communication data, drawing on developing standards and best practice internationally and in the region' (IPPR, 2022, p. 35). The IPPR's findings back up the outcomes of a constitutional assessment from June 2021 on the substance of the new data-retention regulations by the Namibian public-interest law firm, the Legal Assistance Centre (LAC), which similarly concluded:

> Based on the survey of comparative law outlined here, it seems likely that Namibia's telecommunications data retention scheme might be found to be an unconstitutional infringement of the right to privacy overall, given the intrusion into the privacy of large segments of the population in a manner that has a questionable ability to serve the intended objectives (LAC, 2021, p. 22).[6]

It is worth mentioning that the issues raised by the LAC and the IPPR were incorporated into the Namibian civil society shadow report that was submitted to the United Nations Human Rights Committee in February 2024 ahead of the Namibian government's appearance before the committee in early March 2024 for a third periodic review under the International Covenant on Civil and Political Rights (ICCPR). Following the Namibian government delegation's interrogation by the committee, the Human Rights Committee too expressed concern with regard to the new regulations for Part 6 of the Communications Act, stating in their concluding observations, dated 28 March 2024:

> The Committee is also concerned that the data retention regulations currently being implemented for Part 6 of Chapter V of

[6] The Legal Assistance Centre's (LAC) assessment is titled 'Communications Act 8 of 2009: Is the collection and retention of data on telecommunications users constitutional?' and is downloadable from the organisation's website, at www.lac.org.na.

> the Communications Act (No. 8 of 2009) may not provide adequate protections and safeguards for personal communications data. In addition, the implementation of the aforementioned regulations coincides with the implementation of mandatory SIM card registration, raising concerns in particular for persons with a particular need for confidential or anonymous communications such as journalists, whistleblowers, or human rights defenders (Concluding Observations on the Third Periodic Report of Namibia, 2024, p. 8).

The Human Rights Committee recommended that the Namibian government

> . . . ensure that the management of the database for SIM card registration will be subject to appropriate safeguards in order to prevent hacking, data leaks, and unauthorised access by private and state authorities, including appropriate judicial or legislative authorization requirements for state authorities wishing to access the database (Concluding Observations on the Third Periodic Report of Namibia, 2024, p. 8).

This was not the first time that Part 6 of Chapter V of the Communications Act had raised concern at the Human Rights Committee. Back in 2014/2015 the committee raised similar issues, repeatedly questioning the Namibian government's delegation about the alleged unlawful existence of interception centres operated by the NCIS when Part 6 had not been operationalised at the time. This questioning followed testimony before the committee by the Namibian civil society delegation that there was anecdotal evidence that interception centres existed and were unlawfully operational.

This assertion – the alleged unlawful existence and operation of interception centres – has gained credence over recent years, following revelations that around the same time, 2014–6, that the Namibian government was repeatedly denying the existence and operation of such centres before the Human Rights Committee and in correspondence with the committee, during the second periodic review, the Namibian government was actually and actively scouting and procuring sophisticated digital surveillance technologies in international surveillance technology markets (Links, 2019). Similarly, slightly before the second periodic review, in early 2014, a former senior SWAPO parliamentarian explosively and repeatedly claimed in the National Assembly chamber during a parliamentary sitting that the NCIS's surveillance capabilities had been weaponised in internal factional disputes and contestations within the ruling party and that senior party leaders and functionaries' mobile devices were being monitored (Links, 2019). To be clear, these and similar episodes over the years suggested that the types of communications surveillance envisaged and enabled by Part 6 of the Communications Act were already being conducted by the NCIS, wholly unlawfully, given the status of Part 6 at the time.

The foregoing exposition illustrates how authoritarian impulses in contemporary Namibia evince latter-day reproduction of the authoritarian intelligence culture of the liberation-struggle era. This culture has informed the crafting and operationalisation of an authoritarian-style framework for state surveillance in liberal-democratic Namibia. This has happened with no evident pushback from any single formal public-oversight mechanism, specifically the Namibian National Assembly's Standing Committee on Foreign Affairs, Defence and Security, which has traditionally been rather docile in the face of historically overbearing executive power in the legislature. At the same time, as this section also illustrates, it is the indirect, the judiciary, and the informal oversight actors – the media and civil society – that have been active in countering and raising awareness of the significant threats posed by the unaccountability and nontransparency that surrounds the operations and surveillance activities of the NCIS.

The democratic subsidy in Namibia's intelligence oversight

The foregoing discussion shows how Namibia's formal intelligence oversight mechanisms remain weak, thereby creating room for the country's intelligence services to operate outside a structured accountability framework, if not extrajudicially. However, it is arguable that this gap is mitigated by the country's overall democratic infrastructure, which enables some significant degree of informal oversight of intelligence services. The chapter avoids a reductionist argument which conflates lack of formal oversight mechanisms on intelligence services with the broader Namibian polity's democratic profile. It is precisely because of the country's democratic affordances that its intelligence services cannot significantly operate outside democratic parameters and extrajudicially.

Namibia has distinguished itself as a democratic polity in many respects, prominent of which is its profile in terms of freedom of the press, where the country ranks very highly, globally and continentally (Fesmedia Africa, 2022; Freedom House, 2024; Reporters without Borders, 2024). The country's democratic ecosystem is evinced by political pluralism; free, peaceful and credible elections; a free and independent government; expansive civil liberties; associational and organisational rights; the rule of law; as well as personal autonomy and individual rights (Freedom House, 2024). It is this democratic environment that has arguably created conditions for expansive informal intelligence oversight affordances and activities in Namibia. For example, the case of *The Patriot* newspaper shows the multiplier dividend of democratic conditions in the country. The newspaper's ability to investigate corruption within the Namibian Central Intelligence Service (NCIS) was arguably contingent on both the freedom accorded to the press in Namibia and the availability of relevant information in the public domain (Global Freedom of Expression, 2024), which enabled investigative journalist Matheus Haufiku to establish the facts of the case. Furthermore, to its credit, the NCIS itself did not use Gestapo tactics of intimidation to silence the newspaper as would have been the case in typical authoritarian environments. Rather, the merits of the NCIS's arguments notwithstanding, the agency chose a democratic process to make its case against the publication of the story. After losing the case in the high court, the agency appealed the verdict in the supreme court which upheld the outcome of the high court, a ruling that the agency did not reject. This evinces both the social accruals of Namibia's democratic subsidy and the inherence of conflict and contestation in democratic societies.

Moreover, Namibia's democratic subsidy in terms of intelligence oversight is evident in the role performed by civil society organisations and/or think tanks. A prominent example in this regard is the monitorial role being performed by the IPPR. Among other things, it has published several papers on various key public-policy issues, including the operations of intelligence services in Namibia, and has provided critical evaluations of legislative instruments that are aimed at governing intelligence operations and people's rights to privacy in the country, going forward (see Links, 2018, 2019, 2024). The Namibia Media Trust (NMT) has also demonstrated vigilant oversight of Namibia's legal environment regarding intelligence and surveillance activities, as well as the operation of the country's intelligence infrastructure. An example of this is a press statement from the organisation published on 19 June 2018 welcoming the High Court's judgment against the NCIS in the case of *The Patriot* newspaper.

This oversight activity arguably forces the NCIS to operate within the parameters of the national Constitution and laws. In addition, another civil society organisation, the Friedrich Ebert Stiftung, published a study that critically examined the relationship between Namibia's security sector and the state in 2003 (see Du Pisani, 2003). These oversight activities remove the veil of secrecy and mystery from the operations of this sector and provide citizens with insight into the operations of the security sector, in particular the intelligence services, making them more visible and subject to public scrutiny. The public awareness borne of these activities may force the security sector to observe the law and respect the Constitution in their operations.

The surveillance and intelligence scene in Namibia has also been a subject of scrutiny at an international level. For example, an international civic organisation, Privacy International, published a report in 2016 which reviewed threats to privacy rights in Namibia (Privacy International, 2016). This also focused the spotlight on the operations of intelligence services and the legislative instruments that enable such violations in Namibia. Furthermore, organisations such as Freedom House, Reporters without Borders, Afrobarometer, Fesmedia Africa and the African Commission on Human and People's Rights, among others, provide constant oversight of Namibia's state of democracy, which includes analysing the operations of institutions and laws that threaten the fundamental freedoms of citizens, not least the operations of the NCIS. It is imperative to underscore the fact that such oversight activities would be inconsequential in authoritarian societies that mostly disregard democratic institutions and ideas which promote the democratisation of society. Lastly, intelligence oversight in Namibia is arguably occasioned by the country's multiparty democratic dividend. The political contestation that its obtained from political competition is inherently imbued with oversight mechanisms. Namibia is replete with critical voices in the public domain, which include politicians and activists such as Job Amupanda and Michael Amushelelo, among others, who have been freely and fearlessly criticising state institutions thereby providing effective oversight of the latter. Ultimately, it is arguable that democratic societies such as Namibia have a complex and multilayered oversight system which makes the operations of state functionaries such as intelligence services transparent to the citizens, unlike in closed and authoritarian states.

Securing a democratic future in Namibia

As the previous sections illustrate, while formal oversight mechanisms for the intelligence service are deficient and arguably largely failing in their oversight mandate, it has been the informal, nongovernmental mechanisms that have, to some extent, served to provide a measure of effective oversight of the NCIS within the democratic climate established by Namibia's liberal democratic constitutional order. However, as Du Pisani (2003) noted more than two decades ago, there are limits to the type and scope of oversight scrutiny that informal mechanisms, such as civil society and the media, can provide, given the considerable and, to some extent, understandable impervious nature of the governance systems surrounding the NCIS, and to a similar degree the broader state-security sector. Over the last two decades, the resistance to democratic oversight has been progressively entrenched, which is why some have insisted an authoritarian intelligence culture largely pertains in Namibia (Bolliger, 2023). The consolidation of an authoritarian intelligence culture is especially evinced by the introduction and expansion of an intrusive and potentially authoritarian framework for enabling communications and/or digital surveillance by the NCIS since the late 2000s into the early 2020s, as has earlier been demonstrated.

Given this state of affairs, the question that remains centres around how democratic governance of the NCIS can be strengthened, both in terms of fixing and/or filling gaps in the extant legal framework and formal oversight structures with a view to infusing more transparency and impactful scrutiny by informal oversight mechanisms. It is imperative that any and all interventions be geared towards democratising the perduring authoritarian intelligence culture that has been at the heart of this discussion and establishment of a more transparent, accountable and effective culture of intelligence governance that resonates with the liberal democratic values of the Namibian constitutional order. Nonetheless, it is axiomatic that undoing the obtaining authoritarian intelligence culture will not be achieved by simply tinkering with the legislative framework or existing formal oversight mechanisms, but will require the wholesale reform of oversight approaches, including within and among civil society and the media. In this regard, proposed fixes have in some instances been on the table for a long time, while others have emerged quite recently. Some of these fixes are obvious and have been alluded to already.

As Du Pisani (2003) and others (Lindeke, 2007; Tjirera and Hopwood, 2009; Links et al., 2023) have repeatedly pointed out over the years, and in line with the notion of checks and balances immanent to the separation of powers principle, weak legislative oversight over Namibian state entities and departments is ripe for overhaul. In this regard, it is necessary to revisit the long-standing *Agenda for Change* (1995) programme at Namibia's National Assembly, as it provides a road map for strengthening parliamentary oversight of all state offices, ministries and agencies, including the state-security sector. While there appears to be a stated intention and apparent attempts to revive the *Agenda* of late, more urgency is clearly required to breathe life into this democracy-enhancing transformative programme. Regarding intelligence-sector governance, the *Agenda* proposes the installation of an elevated and empowered parliamentary committee system to enhance oversight synergy between the legislature and judiciary, over the executive. This would inevitably mean that the National Assembly's Standing Committee on Foreign Affairs, Defence and Security becomes much more than what it has been to date in terms of holding the security sector, including the NCIS, accountable with regards to the latter's operations and activities.

While these transformations are progressing within the legislature's institutional arrangements, there ought to be a parallel overhaul of the legislative frameworks that speak to intelligence governance. In this regard, as has already been briefly discussed above, the Institute for Public Policy Research (IPPR) proposes specific and significant reform to the communications surveillance governance framework that underpins the NCIS's digital surveillance activities (IPPR, 2022). As previously noted, the NCIS Act of 1997 and the Communications Act of 2009 do not provide for effective democratic governance or oversight of surveillance capabilities and activities. For a way forward, the IPPR's (2022) recommendations would be a good place to start. According to the IPPR (2022, p. 35):

- The framework must be subject to clearer standards of necessity and proportionality, so that communications surveillance may only be conducted on narrowly defined grounds, where necessary for investigations of serious offences and imminent threats to national security or human life, and where less intrusive measures have failed or are not possible.
- The framework should ensure robust and independent judicial oversight of surveillance powers, by providing for specialist judges, with adequate independence and resourcing to fulfil their mandate. The process of judicial oversight must also provide due process for targets of surveillance, in the context of *ex parte* hearings.
- The framework must provide for user notification, in order for people whose communications or communications data are intercepted or accessed to be informed of any potential infringement of their rights so that they can seek recourse.

- The framework must provide for transparent measures across all agencies, oversight bodies and industry stakeholders involved in communications surveillance, including the publishing of regular transparency reports which disclose statistical information about interceptions and access to communications data.
- All standards and safeguards that apply to the interception of communications, inclusive of the recommended reforms, must apply to all forms of communication data, including historical data.
- Policies relating to the storage of communications data and mandatory SIM registration should be withdrawn and reviewed in their entirety, and subject to an evidence-based approach that considers any privacy and data protection risks, the cost of the policy and its impact on digital innovation and connectivity, the capacity and needs of law enforcement and appropriate safeguards and oversight measures.
- These recommendations necessitate wide-ranging amendments to Part 6 of the Communications Act, sections 24-8 of the Namibia Central Intelligence Service Act and the relevant regulations issued under the Communications Act.

Furthermore, something that would significantly complement the implementation of these proposed democratic governance changes or enhancements, according to the IPPR, is the creation of an independent state body or mechanism, such as an inspector general, to specifically monitor the communications surveillance activities of the NCIS. However, it is not just the formal governance or oversight mechanisms that are in need of transformation or reform, for as Du Pisani (2003) noted over two decades ago, the roles of civil society and the media, as well as academia, also require considerable strengthening in terms of providing meaningful public-interest oversight of the state-security apparatus. In this regard, it is necessary to point to the 'key principles of good governance in the security sector', espoused by the UK government's former Department for International Development (DFID), as noted by Du Pisani (2003, p. 4). As these principles posit, for informal oversight mechanisms to play their role optimally, it is necessary that 'an environment exists in which civil society can actively monitor the security sector and be consulted on a regular basis on security policies, resource allocation, and other relevant issues' (DFID, 2000, p. 4). While the Namibian constitutional order adequately establishes such a conducive environment, it is apparent that Namibian civil society, the media and academia are considerably hamstrung by capacity and resource challenges to be able to optimally fulfil their envisaged collective informal oversight mandate. Nevertheless, it is the case that such oversight has been episodically robustly exercised, as highlighted above, which leaves considerable scope for further enhancement.

Conclusion

The question of intelligence oversight, in any context, is fundamentally a question about democracy and the sociopolitical practices, as well as institutions, that both undergird or undermine it. Given the paradoxical position occupied by intelligence services in a democratic society, it is, to use Kant's nomenclature, a categorical imperative that independent, well-resourced, accountable and effective formal oversight mechanisms be embedded in a democratic state's governance structures. From an agonistic pluralist perspective, it is taken for granted that contention over social issues is the quintessential substance of a *bona fide* democracy. As such, not only is there contestation over the substance and structures of existing public institutions and their operations in a democratic society, but such contestations also exist over the rules of engagement in dealing with the former. This chapter has shown that, despite Namibia's status as a constitutional democracy, its formal intelligence oversight infrastructure is deeply flawed and counterintuitive to the country's general reputation as free and democratic. This caveat evidently poses a clear and present danger to the country's state of democracy and the nurturing of active and sovereign citizenship. Be that as it may, not much credit has been given to Namibia's functional and enabling democratic architecture. Arguably, and going by prevalent African standards, the Namibian situation could have been much worse, were it not for its democratic affordances. One of the key areas in which the country's democratic subsidy is evident and functional is in intelligence oversight. On the one hand, rather than use its unaccountability, an economy of secrecy and seemingly carte-blanche powers to create a chilling environment through intimidation, harassment, death threats and outright violence to silence civil society, the media and academia, inter alia, the country's intelligence service, the NCIS, has demonstrated its reverence of the law and democratic institutions. Although there were/are serious objections to the NCIS's arguments in the case of *The Patriot*, it is evident that the agency took the legal course to make its case. The differences over the NCIS's arguments themselves in the court case evince a functioning agonistic democracy, where both the rules of engagement over the resolution of contentious issues and substance thereof, are subject to public contestation. Furthermore, that the case emanated from the activities of non-statal oversight actors evinces the affordances of a free society in which the media and other civic functionaries can operate unencumbered. Without the country's democratic dividend, such oversight would have been very limited, if not non-existent. Ultimately, therefore, we argue that the existence of functional formal and informal intelligence-oversight mechanisms in Namibia and the rest of the African continent is contingent on the existence of a functional agonistic democracy in which social issues are a subject of contested negotiation in the public domain on a daily basis.

References

Absher, S., Grier, R. and Grier, K. 2023. The consequences of CIA-sponsored regime change in Latin America. *European Journal of Political Economy*. 80, p. 102452.

Agenda for Change: Consolidation Parliamentary Democracy in Namibia. 1995. Windhoek, Namibia: Parliament of the Republic of Namibia. [Online]. [Accessed 24 July 2024]. Available from: https://agora-parl.org/sites/default/files/agora-documents/Consolidating%20Parliamentary%20Democracy%20in%20Namibia.pdf.

Aradau, C. and McCluskey, E. 2022. Making digital surveillance unacceptable? Security, democracy and the political sociology of disputes. *International political sociology*. 16(1), pp. 1-19.

Bateman, A. 2016. The KGB and its enduring legacy. *The Journal of Slavic Military Studies*. 29(1), pp. 23-47.

Bolliger, L. 2023. An authoritarian intelligence culture in a democratic state. In: Shaffer, R. ed. *The handbook of African intelligence cultures*. London: Rowman & Littlefield. pp. 473-85.

Caparini, M. 2007/2016. Controlling and overseeing intelligence services in democratic states. In: Born, H. ed. *Democratic control of intelligence services: Containing rogue elements*. London: Routledge. pp. 3-24.

Christians, C.G., Glasser, T.L., McQuail, D., Nodernstreng, K. and White, R.A. 2009. *Normative theories of the media: Journalism in democratic societies*. Urbana: University of Illinois Press.

Communications Act 8 of 2009: Is the Collection and Retention of Data on Telecommunications Users Constitutional? (2021). [online] *Legal Assistance Centre*. Windhoek, Namibia: Legal Assistance Centre (LAC). [Accessed 23 Jul. 2024]. Available from: https://www.lac.org.na/projects/grap/Pdf/constitutionality_of_telecommunications_data_retention_schemes.pdf.

Concluding Observations on the Third Periodic Report of Namibia. 2024. *United Nations Office of the High Commissioner for Human Rights*. Geneva, Switzerland: UN Human Rights Committee. [Online]. [Accessed 23 Jul. 2024]. Available from: https://www.ohchr.org/en/documents/concluding-observations/ccprcnamco3-concluding-observations-third-periodic-report-namibia.

Digital Rights in Namibia. n.d. Windhoek, Namibia: Institute for Public Policy Research (IPPR).

Du Pisani, A. 2003. The security sector and the state in Namibia: An exploration. Friedrich Ebert Stiftung. [Online]. [Accessed 20 Jul. 2024]. Available from: https://library.fes.de/pdf-files/iez/global/04720.pdf.

Du Pisani, A. and Lindeke, W.A. 2009. Political Party Life in Namibia: Dominant Party with Democratic Consolidation. Institute for Public Policy Research. Windhoek, Namibia: Institute for Public Policy Research (IPPR). [Online]. [Accessed 20 July 2024]. Available from: https://ippr.org.na/wp-content/uploads/2010/06/IPPR%20Briefing%20Paper%20NO%2044%20Political%20Party%20Life%20in%20Namibia.pdf.

Fesmedia Africa. 2022. *African media barometer: Namibia 2022*. Friedrich Ebert Stiftung.

Freedom House. 2024. Freedom in the world 2024: Namibia. Freedom

House. [Online]. [Accessed 19 July 2024]. Available from: https://freedomhouse.org/country/namibia/freedom-world/2024.

Gill, P. 2020. Of intelligence oversight and the challenge of surveillance corporatism. *Intelligence and National Security*. 35(7), pp. 970-89.

Global Freedom of Expression. 2024. *Director General of the Namibian Central Intelligence Service v Haufiku*. Columbia University. [Online]. [Accessed 18 July 2024]. Available from: https://globalfreedomofexpression.columbia.edu/cases/director-general-of-the-namibian-central-intelligence-service-v-haufiku/.

Global State of Democracy Initiative. 2024. Namibia. Global State of Democracy Initiative. [Online]. [Accessed 20 September 2024]. Available from: https://www.idea.int/democracytracker/country/namibia.

Goldman, Z.K. and Rascoff, S.J. 2016. Introduction: The new intelligence oversight. In: Goldman, Z.K. and Rascoff, S.J. eds. *Global intelligence oversight: Governing security in the twenty-first century*. New York: Oxford University Press. pp. xvii-xxxii

Gramsci, A. 1957/2021. *The modern prince and other writings*. Paris: Foreign Languages Press.

Held D. 2006. *Models of democracy*, 3rd edn. Stanford: Stanford University Press.

Hillebrand, C. 2012. The role of news media in intelligence oversight. *Intelligence and National Security*. 27(6), pp. 689–706.

Hubbard, D. 2024. What happened to our privacy? Police access to our private data. *The Namibian*. [Online]. [Accessed 19 August 2024]. Available from: https://www.namibian.com.na/what-happened-to-our-privacy-police-access-to-our-personal-data/#:~:text=Three%20new%20provisions%20were%20added,This%20includes%20digital%20data.

Kniep, R., Ewert, L., Reyes, B.L., Treguer, F., Cluskey, E.M. and Aradau, C. 2024. Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies*. 50(1), pp.209-29.

Lichter, A., Loffler, M. and Siegloch, S. 2021. The long-term costs of government surveillance: Insights from Stasi spying in East Germany. *Journal of the European Economic Association*. 19(2), pp. 741-89.

Lindeke, W.A. 2007. *Namibia's Parliament in a Presidential Age: Analysis and Opinion. Institute for Public Policy Research*. Windhoek, Namibia: Institute for Public Policy Research (IPPR). [Online]. [Accessed 20 July 2024]. Available from: https://ippr.org.na/wp-content/uploads/2010/06/IPPR%20Opinion%20No%2021%20-parliament.....pdf.

Links, F. 2018. The rise of the Namibian surveillance state. [Online].

[Accessed 18 July 2024]. Available from: https://action-namibia.org/rise-namibian-surveillance-state-part-ii/.

Links, F. 2019. The threat of unchecked communications surveillance. *Institute for Public Policy Research Democracy report.* 18, pp. 1-32.

Links, F. 2024. *Problematic influences: African national security narratives impacting Namibian cybersecurity and cybercrime law-making*. IPPR.

Links, F., Tjongarero, B. and Shakela, E. 2023. *Revisiting parliament's 'Agenda for Change'*. *Institute for Public Policy Research*. Windhoek, Namibia: Institute for Public Policy Research (IPPR). [Online]. [Accessed 20 July 2024]. Available from: https://ippr.org.na/publication/parliaments-agenda-for-change/.

Melber, H. 2003. Limits to Liberation: An Introduction to Namibia's Postcolonial Political Culture. In: Melber, H. ed. *Re-examining Liberation in Namibia: Political Culture since Independence*. Stockholm, Sweden: Nordiska Afrikainstitutet. pp. 9–24.

Melber, H. 2006. People, Party, Politics, and Parliament: Government and Governance in Namibia. In: Salih, MAM. ed. *African Parliaments: Between governance and government*. Cape Town, South Africa: HSRC Press. pp. 142–161.

Miliband, R. 1990. Counterhegemonic struggles. The Socialist Register. [Online]. [Accessed 17 July 2024]. Available from: https://www.marxists.org/archive/miliband/1990/xx/counterheg.htm.

Mouffe, C. 1999. Deliberative democracy or agonistic pluralism? *Social Research.* 66(3), pp.745-58.

Mouffe, C. 2005. *On the political: Thinking in action*. London: Routledge.

Privacy International. 2016. The right to privacy in Namibia. [Online]. [Accessed 22 July 2024]. Available from: https://privacyinternational.org/advocacy-briefing/734/right-privacy-namibia.

Reporters without Borders. 2024. Namibia. Reporters without Borders. [Online]. [Accessed 18 July 2024]. Available from: https://rsf.org/en/country/namibia.

Saul, J.S. and Leys, C. 2003. Truth, Reconciliation, Amnesia: The 'ex-Detainees'' Fight for Justice. In: Melber, H. ed. *Re-examining Liberation in Namibia: Political Culture since Independence*. Stockholm, Sweden: Nordiska Afrikainstitutet. pp. 69–86.

Saunders, C. 2003. Liberation and Democracy: A Critical Reading of Sam Nujoma's 'Autobiography'. In: Melber, H. ed. *Re-examining Liberation in Namibia: Political Culture since Independence*. Stockholm, Sweden: Nordiska Afrikainstitutet. pp. 87-98.

Security Sector Reform and the Management of Defence Expenditure. 2000. London, UK: Department for International Development (DFID). [Online]. [Accessed 25 July 2024]. Available from: https://securityanddevelopment.org/archive/pdf/DFIDpaper1.pdf.

Shaffer, R. ed. 2021. *African Intelligence Services: Early Postcolonial and Contemporary Challenges*. London: Rowman & Littlefield.

Stackhouse, J.R. 2021. *Enemies of the people: Hitler's critics and the Gestapo*. Cambridge: Cambridge University Press.

Tjirera, E. and Hopwood, G. 2009. *Not Speaking Out: Measuring National Assembly Performance. Institute for Public Policy Research*. Windhoek, Namibia: Institute for Public Policy Research (IPPR). [Online]. [Accessed 20 Jul. 2024]. Available from: https://ippr.org.na/wp-content/uploads/2010/06/Comment%20-%20National%20Assembly%20Performance.pdf.

Wiechers, M. 2010. Namibia's long walk to freedom: The role of constitution making in the creation of independent Namibia. In: Miller, L.E. and Aucoin, L. eds. *Framing the State in Times of Transition: Case Studies in Constitution Making*. Washington, DC: US Institute of Peace Press. pp. 81–110.

World Bank Group. 2021. Poverty and Equity Brief – Africa Eastern and Southern: Namibia. World Bank Group. [Online]. [Accessed 20 September 2014]. Available from: https://databankfiles.worldbank.org/public/ddpext_download/poverty/987B9C90-CB9F-4D93-AE8C-750588BF00QA/AM2020/Global_POVEQ_NAM.pdf.

CHAPTER EIGHT

The challenges of sustaining public oversight: The rise and fall of anti-surveillance activism in South Africa

Jane Duncan

Introduction

This chapter focuses on the rise and fall of anti-surveillance activism in South Africa, from 2010 to date, as a form of public oversight of intelligence-driven surveillance. In 2010 the government attempted to introduce a highly controversial bill, the Protection of Information Bill (Protection of Information Bill, 2010), which threatened to give South Africa's civilian intelligence agency, the State Security Agency (SSA), the powers to overclassify huge swathes of government information and cloak it in a shroud of secrecy: hence, its critics dubbed it the 'Secrecy Bill' (News24, 2011). The campaign against the Bill by organisations such as Right2Know Campaign (R2K), a range of non-governmental organisations (NGOs) outside R2K, the media and the labour movement extracted major concessions from the government. Two successive presidents, Jacob Zuma (president from 2009 to 2018) and Cyril Ramaphosa (president from 2018 to date), failed to sign the Bill into law. Their reluctance to do so was a huge victory for public oversight of state intelligence, and particularly the SSA, which had ultimate responsibility for the Bill.

Activists took this campaign around the 'Secrecy Bill' and broadened it to focus on the reasons why they believed the Bill had come into being in the first place. These reasons included attempts on the part of the Zuma administration to shield from public scrutiny the fact that it was relying increasingly on state intelligence and security institutions and their surveillance capabilities to maintain their grip on power. It also focused more broadly on the ways in which an increasingly authoritarian and exploitative political class globally was using intelligence-driven surveillance to contain dissent against austerity measures imposed in the wake of the 2007–8 global economic crisis and, in doing so, they moved beyond treating surveillance abuses as being exceptional cases involving a few rogue spies, and articulated them rather as systemic features of a failing neoliberal economic system (Right2Know Campaign, 2018b, p. 4). The coalition of organisations that campaigned around the 'Secrecy Bill' then went on to use innovative collective action using more transgressive repertoires of contention (McAdam et al., 2004, pp. 7–8) conducted through campaigns, pickets and protests, underpinned by popular education, documentation and legal advice. They used this momentum to push for greater transparency around incidents, suggesting the state was using surveillance to monitor and even disrupt critics of then President Zuma and the corrupt interests that had coalesced around him, and to force the formal oversight structures to perform their mandated roles of holding the intelligence agencies to account for these abuses.

However, once Zuma was removed as president and replaced by Ramaphosa, anti-surveillance activism shrunk, making it difficult to consolidate the democratic gains made during that period. At the same time, more contained forms of contention, using more well-established forms of claim-making (McAdam et al., 2004, p. 8), such as strategic litigation, has won ground. In 2021, the fight against abusive surveillance culminated in a major legal victory against the government won by the amaBhungane Centre for Investigative Journalism in the highest court in South Africa, the Constitutional Court.

Through the lenses of an emerging body of theory on democratic intelligence oversight and more well-established political process theory, and by synthesising the two in ways that bridge the false dichotomy between top-down (or structural) and bottom-up (or agential) approaches to social change (Dawson and Sinwell, 2012, p. 10), this chapter examines the rise and fall of anti-surveillance activism in South Africa as a form of public oversight. Political process theory in turn draws on several theories, most significantly for the purposes of this chapter, resource mobilisation theory, which seeks to explain the resources that social movements need to mobilise effectively, and political opportunity structure theory, which examines the structural conditions in which social movements are likely to succeed or fail to mobilise (McAdam et al., 2004). These theories are relevant in that they provide basic tools to organise the empirical data. Political process theory provides a framework to examine the potential for what Kniep et al. (2023, p. 2) have referred to as more agonistic forms of oversight animated by more radical understandings of direct democracy as a means of challenging undemocratic surveillance practices, the factors internal and external to public oversight actors that make them likely to succeed, fail or achieve mixed outcomes, and how much autonomy they have in shaping accountability practices around surveillance. By merging these two theories and the analytical frameworks they offer, the chapter answers two main questions: what factors contributed to the rise and fall of the highly effective anti-surveillance activism during Zuma's presidency, followed by the success of strategic litigation? What lessons are to be learnt from this failure and success for emerging practices of public oversight of intelligence-driven surveillance?

This chapter draws on diverse sources of empirical data, including 20 in-depth, semi-structured interviews with the key actors in social movements, NGOs, the media, lawyers, the private sector, government and parliament, declassified SSA documents, parliamentary proceedings and formal inquiries into abuses of the SSA. Ethics clearance was obtained from the University of Glasgow and the University of Johannesburg. Most participants who were interviewed agreed to be named, with a few requesting pseudonymisation. Not all potential participants who were approached for interviews responded positively: notably the SSA and the Presidency did not accede to interview requests. It uses a case-study methodology to explore the main research questions, as it allowed for an in-depth examination of the practice of oversight in its context using a mixed-methods approach (Micova, 2019, pp. 71–84), but with a bias towards interviews.

The campaign against the 'Secrecy Bill' and its evolution into anti-surveillance work

The 2010 version of the 'Secrecy Bill' had its genesis in another Bill introduced to Parliament by then Minister of Intelligence Ronnie Kasrils in 2008, during the Thabo Mbeki administration. His intention was for it to replace the 1982 Protection of Information Act (Protection of Information Act, 1982), which was an anachronism in a democracy in that the then apartheid government used it to maintain inappropriate secrecy about its abuses of basic democratic freedoms. However, his own efforts became controversial in that media and civil society organisations criticised the Bill he introduced for giving the government too much power to overclassify information on national-security grounds, and thereby failing to depart sufficiently from the apartheid-era Act (Parliamentary Monitoring Group, 2008). He withdrew the Bill, leaving the next administration of Jacob Zuma to redraft and introduce the 2010 version of the Bill (amaBhungane Centre for Investigative Journalism, 2010, p. 1).

The 2010 Bill, too, proved to be controversial in that it intended to allow the government to overclassify state information on nebulous national-security and national-interest grounds, and people who disclosed classified information faced stiff penalties for revealing such information (amaBhungane Centre for Investigative Journalism 2010, pp. 1–5). In effect, the Bill threatened to cloak the government in a shroud of secrecy, behind which all manner of self-serving abuses by politicians and government officials became possible. The government department responsible for the Bill was the then newly established SSA. Making it the lead agency in government on information classification gave it the power to extend the kind of secrecy usually reserved for national security matters to other areas of government, the state and even the private sector.

Parliament established an ad-hoc committee to consider the Bill in 2010, dominated by the ruling African National Congress (ANC) and chaired controversially by Cecil Burgess, a former chairperson of the only parliamentary committee that operated in secret as a matter of course, the oversight committee for the state intelligence services, the Joint Standing Committee on Intelligence (JSCI). By that stage, worrying signs had emerged of growing corruption in the government and public service. To cover up signs of corruption, members of the Zuma administration sought to draw a cloak of secrecy over government and state activities by increasing the power of South Africa's intelligence and security services in the country's governance, especially the SSA. Shortly after Zuma took office, his administration established the SSA irregularly by presidential proclamation, rather than through legislation, from an amalgamation of the foreign- and domestic-intelligence branches. This centralisation allowed Zuma to control its intelligence and surveillance capabilities more easily, to monitor perceived political opponents to his (mis) rule, and the Bill would have allowed him even more control over what information reached the public domain (Duncan, 2014, pp. 1–15; Commission of Inquiry into State Capture, 2022, pp. 8–15, 25–30). The Zuma administration also ensured that the JSCI, and the Inspector General of Intelligence, were unable to perform their watchdog roles independently by deploying individuals to these entities that were sympathetic to Zuma. The secrecy around JSCI meetings deprived the public of an important opportunity to participate in oversight by providing ongoing information about the (mis) conduct of intelligence agencies. The only glimpse that they gave into their oversight work was through the release of redacted annual reports via Parliament's National Assembly.

Organised responses to the Bill were extensive and broad-based. Many of the organisations opposed to the Bill coalesced into an information-rights campaign launched in 2010, called the Right2Know Campaign (R2K). It established itself partly as an NGO and partly as a social movement, in that it registered with the government as a donor-funded non-profit organisation, while bringing together a range of social movements through an informal network based on the shared belief in the need for '. . . a society and an international community in which we all live free from want, free from fear, in equality and in dignity' (Right2Know Campaign u.d.(2)), and where the freedom to access and share information contributed to this ideal. R2K attempted to straddle these two organisational forms to galvanise a broad range of social forces together to campaign against the Bill, with its founding statement couched very much in participatory democratic language using 'rights talk' (Madlingozi, 2012, pp. 223–5) – or framing its claim narrowly as a demand for access to the state-created institutions of participatory governance, rather than broadly as a demand to change the state-enabled power relations that thrived on secrecy – to demand the right of access to information as a condition of open, responsive and accountable government (Right2Know Campaign, 2010). Despite the narrow state-centric nature of their demands, these organisations used and transcended well-established and contained forms of opposition typically associated with opposition to legislation (McAdam et al., 2004, p. 7), such as making parliamentary submissions and seeking legal opinions. Rather, they expressed their opposition using a much more diverse protest repertoire, through media commentary, the production and dissemination of popular education materials to explain the problems with the Bill in plain, non-legal language, petitions, community meetings, pickets and protests, as well as street art, culture and film screenings (Voice of America, 2010).

This level of organisation meant that the ad-hoc committee considering the Bill was faced with a wall of criticism of the Bill (Parliamentary Monitoring Group, 2010). However, such was the public pressure that the ANC conceded some of the key criticisms of the Bill (Parliamentary Monitoring Group, 2011). Nevertheless, these concessions did not go far enough for the campaigners (Mabuse, 2011; Smith, 2012). Although some positive changes were made, Parliament eventually passed the still-flawed Bill in 2013, leaving Zuma to execute the final task of signing it into law (Corruption Watch, 2013).

However, the Bill remained unsigned on the desks of two successive presidents, Zuma and Ramaphosa, for a total of seven years, strongly suggesting that neither of them dared to sign it into law out of fear of being taken to court by organisations challenging its constitutionality. Finally, in 2020, Ramaphosa decided to send the Bill back to Parliament to review it and address any constitutional deficiencies it found: a decision that was welcomed by several organisations (Media Monitoring Africa et al., 2020; South African National Editors' Forum, 2020).

In the wake of the successes around the Bill, the campaign extended to the other levers of government power that enabled Zuma's misrule, including anti-democratic uses of the state's surveillance capabilities. R2K, the amaBhungane Centre for Investigative Journalism and other civil society organisations ensured that the selection of a new Inspector General of Intelligence took place in public, after attempts to hold the process in secret. The appointee performs oversight of state-intelligence agencies and has been controversial for lacking structural independence. Parliament has failed to give the Inspector General powers to ensure that its recommendations are binding on the agencies it oversees, leading to the agencies ignoring most of the recommendations. Its budget, staff and information systems are also administered by one of the agencies it oversees, namely the SSA, which creates space for the agency to manipulate these processes to thwart oversight (Duncan, 2022) and leading to accountability gaps widening despite the existence of this office (Gill, 2020, p. 983). The appointment of a candidate that was deployed by the ruling ANC to neutralise the Inspector General was going to compound these problems. So when the time came to select a new candidate, R2K focused its energies on campaigning for the withdrawal of the ANC's preferred candidate for the post, Cecil Burgess, due to his having chaired the JSCI in ways that encouraged excessive government secrecy and unaccountability (Right2Know Campaign, 2016a; Corruption Watch, 2016).

R2K also documented and publicised evidence of surveillance of journalists and activists and assisted them to lay complaints with the Inspector General's office, request investigations and ensure follow-up backed up by legal representation (Duncan, 2022). Much of this evidence related to trade unions, social movements and journalists who had reasonable grounds to believe that they were under either physical surveillance or that their communications were under surveillance (Right2Know Campaign, 2016b; Right2Know Campaign, 2018a). R2K also extended its work into other areas of civic life and democratic space that were under threat (Right2Know Campaign, 2018b, pp. 8–10). By that stage, R2K had moved beyond the purely rights-based approach evident in its founding statement. Suggesting that it has adopted a more radical approach, R2K attributed these abuses to the former president's determination to cling to power, as well as the political elite's need to maintain social control in the face of '. . . a deepening economic and climate crisis accompanied by a rise of right wing populism and authoritarianism' and the political elite's commitment to '. . . a neo-liberal and unsustainable capital driven development path' (Right2Know Campaign, 2018b, p. 4).

One of the organisations affected directly by unwarranted state surveillance was amaBhungane. In 2015, it emerged through a court case involving Zuma that its managing editor, Sam Sole, had been placed under state surveillance from 2008, apparently to establish a source of information he had within the National Prosecuting Authority. The organisation, which had extended its activities beyond investigative journalism and into advocacy for conditions for such journalism, used this revelation to mount a constitutional challenge to South Africa's main surveillance law, the Regulation of Interception of Communications and Provision of Communication Related Information Act (Rica) (Quintal, 2021). While amaBhungane launched the application on its own, several of the organisations that had become central to the mobilisations against secrecy and surveillance applied to become recognised as *amici curiae*, or friends of the court, including R2K.

amaBhungane won its case in the Constitutional Court in 2021, forcing the government to redraft Rica to address its constitutional deficiencies. These deficiencies included the fact that surveillance subjects were never notified that their communications had been intercepted, the Rica judge responsible for granting interception directions to intelligence agencies lacked independence and their process was one-sided in that they only heard the agencies' version of events. The judge was also never informed that the surveillance subject was a journalist or lawyer – who have a professional duty to maintain confidential sources of information – and there was insufficient detail on how the communications that were intercepted were processed. Lastly, the SSA's bulk interception capabilities were operating unlawfully because there was no law authorising this highly invasive surveillance practice (*amaBhungane Centre for Investigative Journalism NPC and another v Minister of Justice and Correctional Services and Others,* 2021). These reforms led to the strengthening of judicial oversight, in that they enhanced the independence and effectiveness of the Rica judge, and public oversight through the provision of information to surveillance subjects confirming surveillance and providing them with the information to contest the bases for surveillance if they were unlawful.

A multifaceted movement: R2K's strategic choices and organising style

R2K made a strategic choice to locate the organisation in what they referred to as progressive civil society: a choice that became more pronounced as the organisation matured. They decided to identify and work with organisations that had a clear social justice agenda, in that they recognised oppression – including through the denial of information – as being inextricably linked to exploitation, and they strove to eradicate both. In other words, they recognised the link between '. . . the inaccessibility and unaffordability that is crucial not only to survival but to the ongoing struggle for equality and justice' (McKinley, 2021, p. 159). R2K also believed that adopting a social-justice agenda necessitated placing working-class voices and issues at the centre of the campaign, as the twin evils of exploitation and oppression was most heavily felt by this social class, which was also least likely to have a voice in policy and legislative debates on these issues. Centring working-class voices necessitated them engaging in working-class-led social movements and local struggles that advanced working-class voices and power (Right2Know Campaign, 2018b, p. 7) and combining popular education with mobilisation, thereby bringing social power to bear on issues through protests, pickets and other forms of social action. At the same time, R2K also wanted to include NGOs that brought technical knowledge around information law and capacity for strategic litigation to the coalition. The organisation's founders recognised that these were likely to be drawn from a social base dominated by the middle class, but they steered clear of an approach that allowed NGOs to dominate.

In taking this flexible and eclectic approach to building the organisation, R2K used what then Interim Programmes Coordinator, Thami Nkosi, referred to as '. . . using the entire toolbox of strategies and tactics, so kind of really doing grassroots work to mobilise ordinary citizens'.[1] Doing so was a logical step for an organisation that was premised on recognising the interconnectedness of struggles for socio-economic transformation and democratic rights such as the right of access to information or the right to privacy free from surveillance. This recognition implied a need for R2K to straddle organisational and social divides that had become all too common in South Africa and transcend the silos in which social problems may be taken up. Nkosi explained:

> What are the weaknesses in civil society organisations or at least social movements in the country? It's just how they create a false dichotomy [in] saying our activism for social justice has no connection with protecting the civic spaces that we operate in. You cannot divorce you fighting for access to sanitation, for example, and staging a protest at the government in a . . . building and being subjected to all kinds of surveillance . . . [And so that], for me, has been the weakness to say we are issue-based, and as a result we don't see just how connected our struggles are.[2]

[1] Interview with Thami Nkosi, interim programmes coordinator, Right2Know Campaign, online on MS Teams, 30 May 2023.

[2] Interview with Thami Nkosi, interim programmes coordinator, Right2Know Campaign, online on MS Teams, 30 May 2023.

Former National Working Group member, Dale McKinley, echoed Nkosi's views. McKinley explained that R2K decided to popularise the Bill and the issues it raised, namely excessive secrecy of information about how power is used and abused in South Africa, and in doing so consciously rejected the temptation to lapse into an organisational approach that relegated the issue to specialist-information rights NGOs. To ensure that social power was brought to bear on the government around the Bill, he argued, R2K needed to take a decision to build what he referred to as a multifaceted movement that consciously sought to straddle the country's massive legacy social divides along the lines of race, class, gender, nationality and geography. McKinley explained:

> I would say first and foremost that the most powerful weapon in my experience . . . is massive mobilisation . . . [You need] collections of activists or community organisations, labour, middle class people, whatever it is. Right2Know was an attempt to do that, and I think it showed for a period of time, it showed what can be achieved when you combine a mass base with advocacy capacity with . . . [the capacity to] do research, the capacity to actually make arguments too, to engage in the battle of ideas, and then also to have a legal component, a legislative component to that, which is to take the state and those that are responsible to task in the court system, pushing for different kinds of changes. In other words [having] a multifaceted movement, that to me has proved to be by far the most effective and [offered] most and strongest possibilities.[3]

R2K adopted a horizontal, federated structure, with a National Working Group (NWG), but with no chair elected at a national conference on a regular basis. The NWG in turn was accountable to branches established in three provinces and coordinating by Provincial Working Groups. However, there was no formal membership:

[3] Interview with Dale McKinley, National Working Group member, Right2Know Campaign, online on MS Teams, 26 May 2023.

Individuals and organisations became involved if they associated with R2K's founding principles set out in its Constitution and elaborated in its national conferences as the organisation's plenary. By 2013, R2K listed 136 organisations as supporters, ranging from residents' associations representing informal settlements and back-yard dwellers to religious organisations and organisations of the unemployed (Right2Know Campaign, 2013). According to former National Coordinator Mark Weinberg, this novel approach to organising meant that the organisation had an energy and vibrancy. Weinberg explained:

> It allowed for a lot of autonomy and gave a lot of space to grassroots activists to kind of set the tone and to present and advance their own issues and their own struggles and didn't impose a bureaucratic, top down, tightly managed attempt to control things. It also unlocked an energy from working class organisations.[4]

Given its commitment to ideological heterogeneity, R2K did not adopt an insurgent or insurrectionary programme, despite its strong base among South African social movements that were more likely to be open to insurgent ideas. Consequently, some of its constituents contested its collective identity, and attempted to narrow it.[5] However, R2K did face distinct challenges in turning surveillance into an issue that gained traction in the organisation. Mass organisations struggling to change how society is organised may well attract intelligence attention and become subjects of surveillance because they are threatening to political elites, and not necessarily because they truly threaten public safety and security. There are clear links between the erosion of democratic rights when surveillance extended far beyond the state's legitimate attempts to protect public safety and security from clear threats, and economic exploitation and

[4] Interview with Mark Weinberg, National Coordinator, Right2Know Campaign, Cape Town, 3 July 2023,

[5] Interview with Dale McKinley, National Working Group member, Right2Know Campaign, online on MS Teams, 26 May 2023.

struggles against it. Nevertheless, R2K still had to expend considerable energy on conducting popular education on state intelligence and surveillance, how it operated and how it was being abused, to create bridges between the problem and the everyday lived realities of its activists. The challenge was compounded by the fact that, as former Secrecy and Securitisation Coordinator Murray Hunter explained:

> Many of the organisations that have been victims of state security abuse were not actually anti-repression organisations. They're not intelligence oversight organisations. They're doing other things and they came under pressure from state security for those reasons, but ultimately their primary mandate is not to fix the spooks.[6]

These difficulties meant that R2K had to undertake 'some delicate work to turn that [surveillance] into a bread-and-butter issue [as] it's pretty far removed from the core kind of work of on-the-ground activism',[7] which meant that much of the technical work around intelligence reform remained separate from R2K's organisational structures of democratic and consultative meetings.[8]

A perennial difficulty of anti-surveillance work is how to ensure that campaigns are built on credible evidence of surveillance, given how secretive intelligence agencies are about operational matters. The problem can lend itself to paranoia, where activists suspect they are under surveillance, when in fact they are not. R2K addressed this difficulty through constant campaigning and popular education, combined with documentation underpinned by legal assistance. The issues gained traction as social-movement activists began to interact with intelligence officers while they were organising protests,

[6] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

[7] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

[8] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

and recognised that they posed a threat to their ability to organise freely, thereby making issues around surveillance and its oversight more concrete.[9]

R2K set about documenting incidents of intelligence harassment of activists and surveillance. They also developed a skill in turning the documentation into complaints that they lodged with the Inspector General of Intelligence, with the assistance of lawyers with knowledge of intelligence and surveillance law. Largely these efforts founded once the complaints were lodged, as the Inspector General failed to make findings on the complaints, although then Inspector General Setlhomamaru Dintwe did try to keep R2K updated on their investigations.[10] R2K also published handbooks documenting stories told by journalists and activists strongly suggesting that the intelligence agencies under Zuma were abusing their surveillance capabilities to monitor and harass his critics. Hunter explained what this slow-burning but systemic process of documenting these experiences and the filing of complaints about them led to:

> It drew these sorts of secret abuses more into the public mind, and I think it probably played a significant part of creating an environment in which there was political pressure to start to clean up a bit. For me, certainly it was a new kind of approach to this problem, which is we document these cases, we try to create a seriousness around it. You know, [what information] feels legitimate enough that we can say this is a finding, and then we go to the oversight body and we submit a complaint and then we start to [push them] for a response. And it ended up running into all the dysfunction of that oversight body and sort of it just died away. But I do think that the work ended up being important, even if it was a very frustrating kind of specific outcome.[11]

[9] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

[10] Interview with Thami Nkosi, interim programmes coordinator, Right2Know Campaign, online on MS Teams, 30 May 2023.

[11] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

R2K aimed to relate these surveillance stories in ways that made connections between individual stories, building up a body of evidence pointing to systematic surveillance abuses. Then they aimed to act on that evidence, attempting to force oversight structures that had become used to operating in secret to respond more openly than they usually did. Despite the lack of response to these complaints, the process of lodging them created pressure on the institution and a focus on its inadequacies and those of the parliamentary institution it was meant to account to, the JSCI.

Cracks emerge in anti-surveillance activism

Cracks began to emerge in R2K, which impacted massively on its ability to continue its distinct style of anti-surveillance activism. The organisation had what Weinberg described as 'self-selecting participation', which meant that individuals or organisations that subscribed to the organisation's mission could become involved with little screening.[12] These participants had the democratic space to bring any issues they wished for inclusion onto its programme, provided they related broadly to the mission, and the organisation's programmatic breadth meant that it was likely that these issues would be taken up. R2K's inclusivity became its Achilles heel, as it suffered from what Hunter described as 'weak organising principles'.[13] R2K became an organisation where '. . . no-one could get thrown out of the room' and '. . . a resting place for people who had been kicked out of every other organisation . . . [or where] their organisation had ceased to exist and they were still coming to meetings . . .'[14]

R2K established itself on the vestiges of social movements established as part of the broader anti-globalisation movement – with

[12] Interview with Mark Weinberg, National Coordinator, Right2Know Campaign, Cape Town, 3 July 2023.

[13] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

[14] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

many activists coming from movements aligned to the Anti-Privatisation Forum[15] – and much of the activist energy that had dissipated from these movements was transferred to the organisation. However, while these movements bequeathed a rich activist legacy that R2K tapped into, the fact that activists were drawn from movements that had declined or even collapsed (Runciman, 2015, pp. 961–79), created accountability challenges as they were not representing clearly defined memberships or constituencies.

Given that the participation model was so poorly defined, friction opened between NGOs tightly accountable to their boards and donors for their activities rather than memberships, and activists drawn from working-class movements with their own organisational challenges. According to former National Working Group member Julie Reid, as internal conflict emerged, NGOs slowly and quietly started filtering out of the organisation:

> A lot of people just didn't have the time, [but] a lot of them, more grassroots activists and community organisations, felt as if they were treated as if they were just the sort of rent-a-crowd. There was a lot of contentious politics within the campaign itself because of these types of relationships. The community organisations . . . [wanted to] be able to express their views as well, and I think a lot of the people from the NGOs and the journalists and the media, they just didn't appreciate that . . . [so there was a lot of] speaking past each other between those two segments.[16]

Neither was R2K able to turn to more well-established social movements, such as the trade-union movement, for a more well-structured participation model, where activists represented clearly defined constituencies and could be recalled by those constituencies if they failed to do so adequately. Trade unions proved to be the most

[15] Interview with Dale McKinley, National Working Group member, Right2Know Campaign, online on MS Teams, 26 May 2023.

[16] Interview with Julie Reid, former National Working Group member, Right2Know Campaign, online on MS Teams, 1 August 2023.

difficult to organise, despite R2K having documented evidence of them being under surveillance by Zuma's SSA. For Hunter, this was due to them being '. . . busy, chaotic and under intense political pressure. [The unions that were the most targeted] were also the unions that seemed to have the most problems with internal democracy.'[17] This problem meant that these unions were least able to mount an organised response as they were unable to transcend their own internal divisions.

In the absence of a broader social movement that 'lifted all boats' in Weinberg's words,[18] R2K was forced into becoming that movement. Expectations piled up at its door in the wake of its successful campaign against the Secrecy Bill as it had developed an image publicly of being effective and was taken seriously by political elites. Consequently, its participation model came to rest more heavily on its own structures, anchored by its staff that were drawn increasingly from the organisation's activist base. The intention of doing so was a well-meaning one, namely, to recognise activists who had stayed the course in the organisation and remunerate them for their participation. However, in conditions of an unemployment crisis affecting the working class disproportionately, employment of a few activists while others remained unremunerated became a source of considerable friction, injecting the organisation with what Weinberg referred to as the 'politics of survivalism'.[19] R2K became '. . . an organisation whose primary objective was to self-replicate, which meant that the work that was happening was happening outside the democratic structures, as it had been crowded out by the internal discussions.' This happened because these increasingly toxic dynamics '. . . led to the organisation spending an extraordinary amount of time talking about its own structures'.[20] To address the very real challenges activists had in remaining

[17] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

[18] Interview with Mark Weinberg, National Coordinator, Right2Know Campaign, Cape Town, 3 July 2023.

[19] Interview with Mark Weinberg, National Coordinator, Right2Know Campaign, Cape Town, 3 July 2023.

[20] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

engaged as volunteers, R2K began to offer stipends for transport, air time and other expenses. However, doing so came with its own challenges, in that it created a perverse incentive to participate simply to claim the stipend (Right2Know Campaign, 2018, pp. 15–16).

What Hunter described as 'insufficient internal housekeeping' in a misguided attempt to achieve 'pure democracy' led to a situation where 'people weren't there for the same reasons'.[21] R2K's programme became an accumulation of struggles that were increasingly difficult to relate to the core mandate, which itself had ballooned, as too few tough choices were made about which issues were included on the agenda. These problems became increasingly toxic and led to tensions developing along the lines of race, class and gender. Nkosi felt that some staff members were subjected to 'vile attacks' as they were remunerated for their work while activists were not, and in-fighting led to R2K being reduced to a media campaign, with less and less organising on the ground taking place.[22] As Nkosi explained:

> What then happened is that the struggle for resources, I mean we can't divorce the Right2Know, we are just a microcosm of what the society is in this country with the high levels of unemployment, lack of access to resources, inequalities and everything else. That played itself out within the Right2Know Campaign.[23]

Meeting agendas became crowded with too many items, and R2K's success in fundraising, coupled with the fact that some key donors were interested in social movement-building in an environment where there were fewer and fewer movements to fund, meant that there was little financial incentive to pare back.[24]

[21] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

[22] Interview with Thami Nkosi, interim programmes coordinator, Right2Know Campaign, online on MS Teams, 30 May 2023.

[23] Interview with Thami Nkosi, interim programmes coordinator, Right2Know Campaign, online on MS Teams, 30 May 2023.

[24] Interview with Mark Weinberg, National Coordinator, Right2Know Campaign, Cape Town, 3 July 2023.

In 2019, the presidency declassified a report drawing on information brought forward to an investigation by whistleblowers in the SSA, confirming that the SSA had put R2K and other NGOs and social movements under surveillance, and a subsequent declassified SSA report detailed how it had paid sources to masquerade as activists in these organisations (State Security Agency 2017; Mufamadi, 2018). The report suggested that potential allies in the fight against unaccountable surveillance had emerged in the SSA in the form of the whistleblowers who were themselves concerned about surveillance abuses and these exposés within the SSA provided a democratic opening for activists to escalate their struggle. However, by that stage, R2K was in such a weakened state that the revelations deepened internal tensions, in that it created a whispering campaign about who in the organisation had acted as paid SSA agents. It did galvanise the organisation into action in that it started to screen who became involved. According to National Working Group member Bongani KaMthembu, they tried to '. . . tighten up the entrance of whoever comes. It's no longer an open book like before'.[25] However, by this stage the organisation was in a downward spiral that it has not recovered from. Its decline has meant that the anti-surveillance work has to be taken up by other organisations that remain in a stronger position to do so. At the forefront of these efforts was the investigative journalism centre and one of the founders of R2K, amaBhungane.

Strategic litigation overtakes anti-surveillance organising: The amaBhungane Constitutional Court case

amaBhungane's challenge to the constitutionality of Rica was underpinned by a very well-planned and well-executed legal strategy, or as Hunter put it, a 'practical scaffolding that led to an outcome'.[26]

[25] Interview with Bongani KaMthembu, National Working Group member, Right2Know Campaign, 29 May 2023.

[26] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

The case was the culmination of what Nkosi described as a 'beautiful journey', where strategic litigation built on the anti-surveillance momentum started by R2K to force the government to reconsider its inadequate privacy protections in Rica.[27] The path from the anti-surveillance organising of R2K to strategic litigation was not a smooth one, however, with the latter overtaking the former as a strategy to continue the fight against unwarranted surveillance.

Possibly the most important factor that led to the success of the case was that the organisation had clear, irrefutable evidence, in the form of a court transcript, that its Managing Editor Sam Sole had been put under surveillance by the state. He was not the only journalist to make this discovery. Two former journalists from South Africa's largest weekly newspaper, the *Sunday Times*, Mzilikazi wa Afrika and Stephan Hofstatter, learnt that the Crime Intelligence Division of the South African Police Service (SAPS) had put them under surveillance to identify their sources of information, and they were tipped off by their sources as to this fact (Duncan, 2014, pp. 224–7). Evidence then emerged through a labour court dispute that confirmed the surveillance. Other journalists also learnt of surveillance through tip-offs (Right2Know Campaign 2018a), but they struggled to take material steps as they were difficult to organise as a group, even though their surveillance '. . . fell quite easily into the narrative of repression in the early 2010s'.[28]

amaBhungane was, however, able to take steps because they had the funding networks to raise funds for the case, and a legal network willing to represent them at reduced, non-commercial rates. They also ploughed any recovered legal fees from cases they won back into more litigation.[29] Another factor was that amaBhungane's founders, Sole and Stefaans Brümmer, had taken a deliberate decision at their launch in 2010 – the year of R2K's establishment – to

[27] Interview with Thami Nkosi, interim programmes coordinator, Right2Know Campaign, online on MS Teams, 30 May 2023.

[28] Interview with Murray Hunter, former Secrecy and Securitisation Coordinator, Right2Know Campaign, online on MS Teams, 2 June 2023.

[29] Interview with Sam Sole, Managing Editor, amaBhungane Centre for Investigative Journalism, online on MS Teams, 14 July 2023.

depart from a conventional, positivist journalism of observation associated typically with the professional model of journalism and commercial media operations. Instead, they embrace a public journalism model with an advocacy component or, more specifically, accountability journalism, and their status as a non-profit journalism organisation gave them the space to do that. In doing so, they aimed to practise what Brants and de Haan (2010, p. 418) have referred to as empathetic responsiveness, where journalists side with a traditionally voiceless public and act as advocates of their cause to public authorities that included an advocacy component. The purpose of the advocacy was to ensure conditions for independent investigative journalism through defending and promoting information rights. Thus, 2010 was a period of innovation, with innovators experimenting with new organisational forms. The advocacy component of amaBhungane's work – which included pursuing access to information requests, litigation on information rights and submissions to various public bodies – had to be managed very carefully to ensure that it did not compromise the independence of the journalism, but for Sole, if one embraced a public journalism stance, then the two activities were not contradictory but complementary:

> So, this was a brainchild of Stefaans and I and from the beginning. It was always conceived as being based on three legs, one being trying to do best practice investigative journalism. Two being trying to transfer some of the skills and knowledge and so on. So, training and sharing or skills transfer, that being the second leg and the third leg being advocacy. [Investigative journalism] is essentially . . . quite campaigning journalism. It's accountability journalism. It has a particular moral standpoint, I suppose . . . [advocacy] and journalism has fed into one another. We handled the potential conflict by keeping the two separate, with the advocacy person not being a journalist . . . [and] we clearly distinguish between the two in publications.[30]

[30] Interview with Sam Sole, Managing Editor, amaBhungane Centre for Investigative Journalism, online on MS Teams, 14 July 2023.

amaBhungane contributed to R2K's establishment to achieve the objective of building more of a mass base for its work, and the advocacy coordinator represented amaBhungane on the National Working Group. However, the growing number of issues that R2K dealt with made it increasingly difficult for them to remain engaged in the organisation's leadership, and they stepped down from this role. This experience led Sole to conclude that they did not really have the capacity to be involved '. . . in something that was trying to be more of a movement, and so I think we've stuck to that'.[31]

The model of an investigative journalism centre contributing to an organisation that had some characteristics of a social movement worked well for a while. It allowed them to contribute to the victory around the Secrecy Bill, and to raise the profile of the campaign work around the independence of the Inspector General. This office had become a serious concern to amaBhungane because it was not willing to confirm or deny the existence of a surveillance operation against Sole, even though evidence had emerged of such, and highlighted its lack of robustness.

amaBhungane's attorney on the Rica case, Dario Milo, was used to operating on brief for clients and less familiar with aligning legal strategies with movement campaigns led by multiple actors that at times disagreed with one another. Nevertheless, he was pleasantly surprised by what he described as the vigorous and relentless campaign of civil society and the media – involving marches and protests and other forms of mass action – had the effect it did, and it was not just the legal submissions that were relied on to stop him from adopting the Bill.[32] Also heartening was the fact that Ramaphosa's legal team had indicated that it was open to a legislative review of the most problematic areas of the Bill and signalling a different approach to the Bill as compared to the previous administration. Milo said:

[31] Interview with Sam Sole, Managing Editor, amaBhungane Centre for Investigative Journalism, online on MS Teams, 14 July 2023.

[32] Interview with Dario Milo, media lawyer, online on MS Teams, 17 July 2023.

> [Legal victories like Rica and the Secrecy Bill] depend upon a broad Church of like-minded organisations and media companies, who can collectively come to court to say, this isn't just an amaBhungane problem, or a Mzilikazi wa Afrika being surveilled problem. It is a systemic issue that affects the whole [journalism] industry, and that certainly played a huge role, I think, in the success against the Secrecy Bill . . . is that collective sense of we're in this together. [The court transcript confirming the surveillance of Sole and the non-committal response of the Inspector General] and being able to put all of that in a court application, I think certainly created the right atmosphere and conditions for a court to say this is a real problem.

The fact that the case occurred in an international moment, when state surveillance overreach was a major public issue following the abuses revealed by former National Security Agency contractor Edward Snowden, also worked to the advantage of amaBhungane and its legal team. It meant that it had available to it progressive international jurisprudence on surveillance reform, and organisations that had contributed it could be drawn on to contribute their expertise. One of those was London-based but international advocacy organisation Privacy International, which became a Friend of the Court in the amaBhungane case. Programme Director and Senior Legal Officer Ilia Siatitsa explained:

> It goes without saying it's a landmark judgement that we have. It has been a great honour to even be a small part of [it]. In my view, one of the biggest achievements of the case as such to begin with was that it forced the government to admit to the existence of the [SSA's] bulk interception programme to begin with, it was not in the law and there are very few governments in the world . . . [That] is great.[33]

[33] Interview with Ilia Siatitsa, Programme Director and Senior Legal Officer, Privacy International, online on MS Teams, 14 July 2023.

Analysing the findings through a synthesis of oversight and political process theories

This section uses the emerging literature on democratic oversight, synthesised with political process theory, to explore how public oversight of intelligence-driven surveillance has been organised in South Africa, to what end and its impact. Political process theory seeks to explain the conditions under which social movements are likely to succeed or fail to achieve their objectives. These conditions include the extent to which a political system is open or closed to challenge, the extent to which this system is stable or unstable, the availability of potential allies, leading to the formation of new alliances and greater political empowerment, and conflict among the elite (McAdam et al., 2004, pp. 3–72). A synthesis of the two allows for an examination of factors that are both internal and external to movements and their impact on movement success or failure. For the purposes of this analysis, R2K is being understood as a social movement, although as explained earlier, this characterisation is not without its problems.

The anti-surveillance activism discussed in this chapter qualifies as public oversight of intelligence-driven surveillance, and democratic oversight at that. The activism started out initially as a popular campaign against the 'Secrecy Bill', organised partly under the rubric of R2K, and escalated into an information-rights campaign with multiple legs. One of these legs focused on abuses of the security and intelligence apparatuses of the state, including its human and digital intelligence and surveillance capabilities. In articulating the problems, it was campaigning around as part of a broader systemic attack on progressive and popular democratic social forces (Right2Know Campaign 2018b, p. 4), increasingly R2K adopted a critical approach, moving beyond individualising and exceptionalising surveillance abuses and explained them as being a by-product of an exploitative and oppressive neoliberal economic system (Choudry, 2018, p. 3–16). While there was a strong element of 'rights-talk' (Madlingozi, 2012, pp. 222–39) in the campaign, they also broadened their analysis of pervasive secrecy and surveillance into a critique of neoliberalism. In doing so, they appealed to a broad range of social forces across South Africa's myriad divides. They also moved beyond a narrow programme of oversight reforms that were vulnerable to reversal, by articulating the problem as one that would require lasting solutions that dismantled the root cause of the problem of growing authoritarianism, namely inequality. By the time amaBhungane took over the leadership of the anti-surveillance work, the conception of the problem narrowed again from a focus on a broader socio-political critique to the chilling effect of surveillance on investigative journalism and information rights as the lifeblood of such journalism (Quintal, 2021; Thakur, 2021). Nevertheless, its non-profit status allowed amaBhungane to operate with a conception of journalism that was public-facing and took its practices far beyond positivistic conceptions of the journalism of observation, and which allowed it to play this leadership role in ways that benefited broader society.

As discussed in the introduction (Duncan and Munoriyarwa, this volume; Caparini, 2007, p. 3), intelligence oversight could be understood as the superintendence of intelligence in a manner that is independent from the everyday management and practices of intelligence and the institutions that collect, analyse and store it. Conventional accounts of intelligence oversight would reduce oversight to the practices of formal oversight structures – which in the case of South Africa were the JSCI, the Inspector General of Intelligence, the executive arm of government and the judiciary – and this chapter shows that it was precisely because of the deficiencies, including the lack of independence, of these structures that anti-surveillance activism as a form of public oversight became necessary. The participating NGOs, media organisations and social movements supervised the intelligence agencies by documenting and publicising what they believed to be unlawful surveillance, laying complaints and requesting investigations, providing a voice for surveillance victims and campaigning for greater independence of the formal oversight bodies they were forced to compensate for. The 2016 campaign for a transparent and independent appointment process for the Inspector General led to the withdrawal of the ANC's preferred candidate and public (as opposed to secret) hearings for all candidates: a major victory of public oversight. The publicised cases of surveillance abuses did not result in meaningful redress for the victims, however, until amaBhungane launched its legal challenge. This case led to a major court victory with lasting, positive, international repercussions, in that it forced the government to rewrite the law, after having dragged its feet on legislative reforms for years, and setting an international legal precedent that other courts could draw on.

The South African case study amplifies a finding in the public-oversight literature that oversight innovations tend to occur, not necessarily in the ordinary course of events when stasis is likely to set in, but when activists use surveillance scandals to force the formal structures to change how they operate through public pressure, and after the responsible agencies have been delegitimised. These scandals become the real moments when intelligence oversight is practised (Kniep et al., 2023, p. 2). However, they also carry with them the risk that the oversight innovations that the scandals unleashed become institutionalised and, ultimately, neutralised though the establishment of 'legitimate' formal bodies and enabling laws that revert to minimalistic oversight once the scandal has died down. With regards to the particularistic verses generalising nature of the injustices claimed by the anti-surveillance activists (Aradau and McCluskey, 2022, pp. 1–19), amaBhungane pursued a particular complaint about one of its investigative journalists and journalists in general, which led to a court ruling adopting special defences for this occupation. However, the more generalised claims made by R2K about surveillance being part of a broader neo-liberal attack on democracy that necessitated a change in direction of the government's economic policies, failed to gain sufficient traction to force change. Consequently, the judgment could be institutionalised in the formal oversight structures more readily, although it cannot be said that its effects were neutralised: on the contrary, the legal case pushed the institutions to innovate and led to enduring, positive changes to the practices of formal oversight over surveillance.

However, the conceptions of the public and of democracy that galvanised this activism were contested and these contestations remained unresolved and an area of considerable weakness. Anti-surveillance activists clearly took democracy seriously and pursued an ideal of ‘pure democracy’, or horizontalism, involving a conscious rejection of hierarchy with leaders at the apex, although not to the point of eschewing an elected-leadership structure altogether. Consequently, they experimented with novel organisational forms that enabled more radical forms of direct democracy, or the right to engage through non-institutionalised channels such as protests – and in situations where representative democracy had failed to deliver robust oversight. In doing so, they drew on South Africa’s longer history of public protests to confront political elites, by mobilising the residual social-movement networks that still existed. In any event, parliament and government had limited the scope for participatory democracy relating to intelligence oversight by ensuring that parliamentary oversight took place largely in secret.

These activists attempted to transcend the socio-economic divisions in society and achieve a more inclusive definition of the public and how it was constituted for oversight. Such divisions had translated into schisms between mass-based, working-class social movements that may be relatively resource-poor and NGOs with expertise in litigation and policy advocacy, but with a social base typically limited to the middle class and with no real membership to speak of, but with access to donor funding. The case study exposes the difficulties of doing just that, and how activists were unable to sustain mobilisation around oversight practices as a result, leading to a conscious choice to reduce mobilisation efforts, limit the terms of engagement with the state and focus on litigation to keep the momentum going. The publics that were galvanised included media organisations, NGOs and social movements, but less so trade unions, and the relationship to the social movements that were mobilised through the campaign against the Secrecy Bill were difficult to sustain. However, even though R2K emphasised physical rather than digital networking – which meant that activists created stronger ties with one another than would have been possible had the organisation used a digital campaign – the organisation also suffered from the weaknesses of horizontalism, namely a lack of structure that created a vacuum that progressive forces were ill-equipped to take advantage of (Bevins, 2023). Not having a clearly defined membership with the right to recall and a tightly defined mandate opened the organisation up to being pulled in too many different directions, and interpersonal conflict that, at times, was amplified by existing race, class and gender divisions, and opportunism.

The reasons for the faltering activism need to be understood in the broader national and global context, where the political system becomes more hostile and closed to challenges. The establishment and ultimate decline of R2K mapped over onto the rise and decline of social movements opposed to neoliberal globalisation in the early 2000s, or what Bevins has referred to as the mass-protest decade from 2010 to 2020 (Bevins, 2023). A new wave of social movements sprung up in the wake of the 2007–8 world capitalist crisis, triggered by persistent greed-induced overlending by United States financial institutions. This financial crisis was felt globally and led to increasing unemployment and homelessness, triggering opposition movements to the austerity political elites around the world imposed to stabilise the crisis. Those movements too declined as they were crushed systematically through police action or they unwound due to their own internal problem (Satgar and Williams, 2021; Bevins, 2023). While it worked impressively for a time, R2K's participation model failed to take these weaknesses into account sufficiently, forcing it to overcompensate for these weaknesses by attempting to become a social movement itself. However, without a clearly defined constituency and in a context of diminishing resources among the social base it organised, the resources it attracted became the focus of deep internal divisions that it was unable to transcend.

Another factor that presented an opportunity for anti-surveillance activism related to the divisions in the political elite and, specifically, the divisions in the ANC between Zuma and his supporters and Ramaphosa and his supporters. There can be little doubt that these divisions created an opening for surveillance reform, building on the victory around the Secrecy Bill. At the time of this contest for control of the ANC, the political system became unstable, but not necessarily to the point of significant political realignments in the form of new and significant political contestants. The ANC remained in power, albeit with a reduced majority, and stabilised once Zuma's contest for power was neutralised. The Zuma presidency lost the political will to sign the by-then hugely controversial Secrecy Bill into law. Neither was Ramaphosa willing to do so, and in fact he indicated his intention to review the Bill. This is a legacy of R2K and allied organisations and left an information-rights movement in its wake that for a time galvanised a broad cross-section of South African society across the country's multiple social divides. Public perception, buoyed by media support for the campaign and opposition to Zuma's rule for its persistent attacks on media freedom, created conditions for heightened public oversight. This is because it fuelled a climate of profound mistrust in state intelligence and its surveillance capabilities, leading to the 'narrative of repression', as Hunter described it, dominating public discussions about intelligence and surveillance, as these capabilities became tainted and ultimately delegitimised by the Zuma administration's abuses for narrow political and corrupt purposes.

As abusive surveillance affected the highest levels of government, allies in the fight against such surveillance began to emerge in the intelligence agencies themselves. These events triggered an investigation informed by whistleblowers inside the SSA with insider knowledge of intelligence abuses against Ramaphosa's leadership bid, and political and society and social movements who were critical of the Zuma administration, followed by legislative reforms to disestablish the SSA and strengthen intelligence oversight: reforms that were unlikely to have taken place had it been ordinary political activists who were surveilled. The Constitutional Court case also forced reforms of Rica, which strengthened judicial oversight and created the potential for heightened public oversight through the user notification requirement. They also led to a formal oversight system that was forced to become more sympathetic to criticisms of abusive surveillance, including the Inspector General of Intelligence and JSCI. Communications companies that are legally obliged to enable state surveillance, found it more difficult to sustain this role uncritically as abuses received more publicity, heightening the risk that they would become tainted with the associated controversies.

However, there are indications that these reforms are likely to be superficial, and not lead to substantial democratic openings. During the legislative reforms that followed the investigation initiated by Ramaphosa in the wake of the surveillance revelations, the mandates of domestic and foreign intelligence were expanded to include a focus on national security interests and not just national security threats. Furthermore, in the wake of destabilising riots in parts of South Africa in 2021, Ramaphosa absorbed the SSA into the presidency and removed the Minister of Intelligence position, leading to a weakening of executive oversight: a problem acknowledged by the chairperson of the JSCI. These constraints to the oversight innovations that were won through activism followed by strategic litigation, strongly suggest that the democratic spaces for intelligence reform that have opened may close, unless there is a sustained public effort to keep them open.

Conclusion: The right people in the right room with the right agenda

In 2018, R2K conducted an evaluation and mid-term review of the organisation. Both pointed to some key changes the organisation needed to make to maintain its momentum and prevent further decline. While the organisation had focused, correctly, on uniting progressive civil society and enabling broad-based participation, its participation model needed to change. The review and the evaluation floated a suggestion that was never implemented, namely, to restructure the organisation away from the provincial working groups that formed the engine room for participation. In their place, they proposed establishing Campaign Action Teams (CATs) around specific themes that aimed to 'get the right people in the right room with the right agenda' (Right2Know Campaign 2018, p. 13). The CATs would bring activists together in a more focused way on specific issues they cared about, such as surveillance, to enable depth of discussion, while drawing on the full range of capacities in the activist base. Priorities would be identified at national level and worked into provincial programmes of action at local level, with periodic meetings of all the CATs to ensure that silos did not develop.

The criteria for participation in the CATs were much more clearly defined than R2K's then model, as they included activists with a mandate to represent mass-based organisations or with a proven capacity to draw over 50 people to a meeting, as well as activists – either representing an organisation or an individual – with useful skills and willingness to contribute these to R2K. While no agreement was arrived at on what the voting power of the second category of members would involve, what was agreed upon was that the organisation needed to include new members with the support of 60 per cent of the existing membership, keep a record of members, audit them regularly and remove members that did not meet the criteria. This new approach would mean working in fewer communities and on fewer issues but doing so in a deeper way (Right2Know Campaign 2018, pp. 11–15; Community Development Resource Association 2019, pp. 21–3).

The proposal for the establishment of CATs – which distil the learning of anti-surveillance activism into an organisational form that could be of more general application beyond the South African case and that, therefore, is useful for thinking through a model for enabling, defining and steering participation in public oversight – came too late to arrest the decline of R2K, but they appeared to strike a balance between the seemingly conflicting priorities of expanding participation while sharpening focus and narrowing programmes, defining membership and increasing accountability. They avoided the dangers of 'pure democracy', or horizontalism, and 'rent-a-crowd' approaches, while recognising that broad-based participation was necessary for the campaign to exercise social power. They offer salutary lessons for future attempts at public oversight of intelligence-driven surveillance and provide tools to make it more sustainable. These strategies could help to protect anti-surveillance work somewhat from harassment by the state and private actors supportive of surveillance, and in conditions where political spaces are closing. They could also create the organisational agility to build on openings when they present themselves in the state and private sector, and where sympathetic individuals identify with criticisms of surveillance measures.

These strategies could also insulate more mass-based forms of oversight from the ebbs and flows of social movements in the wake of the mass-protest decade, when mass movements are likely to be weaker. They also offer a clearly defined but still broad-based participation model for public oversight that could bring into the same room social movements, NGOs, lawyers and journalists committed to public journalism, and keep them there. These participants could then contribute the best of what they have to offer based on solidarity and mutual respect, but united by a shared moral belief that a democracy free from unwarranted surveillance necessitates a fairer distribution of wealth and resources. What is clear from the case study, though, is that retreating from more participatory approaches to anti-surveillance work is not an option; rather, the challenges, complexities and contradictions of engaging in movement building should be embraced. As the evaluation concluded on a note that related to R2K, but that holds true for building a model for successful and sustainable public oversight of intelligence-driven surveillance, 'This is new territory and there are no readily available answers but to keep the questions and learning alive' (Community Development Resource Association, 2019, p. 22).

References

amaBhungane Centre for Investigative Journalism. 2010. *Briefing note: what's wrong with the Protection of Information Bill*. [Online]. [Accessed 9 May 2024]. Available from: https://serve.mg.co.za/uploads/2010/09/01/briefing-notewhats-wrong-with-the-protection-of-information-bill.pdf.

amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v amaBhungane Centre for Investigative Journalism NPC and Others (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) (4 February 2021). [Online]. [Accessed 29 May 2024]. Available from: https://www.saflii.org/za/cases/ZACC/2021/3.html.

Aradau, C. and McCluskey, E. 2022. Making digital surveillance unacceptable? Security, democracy, and the political sociology of disputes. *International Political Sociology*. 16, pp. 1–19. [Online]. [Accessed 20 July 2023]. Available from: https://doi.org/10.1093/ips/olab024.

Bevins, V. 2023. *If we burn: the mass protest decade and the missing revolution*. New York: Public Affairs.

Brants, K. and de Haan, Y. 2010. Taking the public seriously: three models of responsiveness in media and journalism. *Media, Culture & Society*.

32(3), pp. 411–28. [Online]. Available from: https://doi-org.ezproxy2.lib.gla.ac.uk/10.1177/0163443709361170.

Caparini, M. 2007. *Democratic control of intelligence services: Containing rogue elephants.* Aldershot: Ashgate.

Commission of Inquiry into State Capture. 2022. Judicial commission of inquiry into state capture report: part V: vol. 1: State Security Agency and Crime Intelligence. [Online]. [Accessed 29 May 2024]. Available from: https://www.saflii.org/images/state-capture-commission-report-part-5-vol1.pdf.

Corruption Watch. 2013. Secrecy Bill passed by Parliament (press statement), 26 April. [Online]. [Accessed 10 May 2024]. Available from: https://www.corruptionwatch.org.za/secrecy-bill-passed-by-parliament/.

Corruption Watch. 2016. Little transparency in Parly shortlist process (blog), 28 April. [Online]. [Accessed 13 May 2024]. Available from: https://www.corruptionwatch.org.za/little-transparency-parly-shortlist-process/.

Dawson, M. and Sinwell, L. 2012. Transforming scholarship: Sober reflections on the politics of resistance. In: Dawson, M. and Sinwell, L. *Contesting Transformation: Popular Resistance in Twenty-first Century South Africa*. London: Pluto Press, pp. 1–22.

Duncan, J. 2014. Communication surveillance in South Africa: the case of the *Sunday Times* newspaper, in Association for Progressive Communications. Global information society watch 2014. [Online]. [Accessed 27 May 2024]. Available from: https://www.giswatch.org/sites/default/files/communications_surveillance_in_south_africa.pdf.

Duncan, J. 2022. State intelligence mess: how the SA watchdog's teeth have been pulled. *Daily Maverick*, 23 January. [Online]. [Accessed 23 May 2024]. Available from: https://www.dailymaverick.co.za/article/2022-01-23-state-intelligence-mess-how-the-sa-spy-watchdogs-teeth-have-been-pulled/.

Duncan, J. 2022. South Africa's intelligence watchdog is failing civil society. How to restore its credibility. The Conversation, 30 November 2022. [Online]. [Accessed 13 May 2024]. Available from: https://theconversation.com/south-africas-intelligence-watchdog-is-failing-civil society-how-to-restore-its-credibility-195121.

Gill, P. 2020. Of intelligence oversight and the challenge of surveillance corporatism. Intelligence and National Security. 35(7), pp. 970–89. doi: 10.1080/02684527.2020.1783875.

Kniep, R., Ewert, L., Reyes, B., Tréguer, F., Cluskey, E., and Aradau, C. 2023. Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies,* pp. 1–21. doi:10.1017/S0260210523000013.

Mabuse, N. 2011. South Africa's assembly passes 'state secrets' law. *CNN World,* 23 November. [Online]. [Accessed 10 May 2024]. Available from: https://edition.cnn.com/2011/11/22/world/africa/south-africa-state-secrets/index.html.

Madlingozi, T. 2012. How the law shapes and structures post-apartheid social movements: case study of the Khulumani Support Group. In: Dawson, M. and Sinwell, L. eds *Contesting Transformation: Popular Resistance in Twenty-first-Century South Africa*. London: Pluto Press, pp. 222–39.

McAdam, D., Tarrow, S. and Tilley, C. 2004. *Dynamics of contention*. Cambridge: Cambridge University Press.

McKinley, D. 2021. Democracy and the right to know in South Africa. In: Williams, M. and Satgar, V. eds *Destroying democracy: neoliberal capitalism and the rise of authoritarian politics*. Johannesburg: Wits University Press, pp. 148–62.

Media Monitoring Africa, amaBhungane, Right2Know and SANEF and Ronnie Kasrils. 2020. Secrecy Bill is still flawed and needs to be reconsidered. *Daily Maverick*, 9 July. [Online]. [Accessed 10 May 2024]. Available from: https://www.dailymaverick.co.za/article/2020-07-09-secrecy-bill-is-still-fundamentally-flawed-and-needs-to-be-reconsidered/.

Micova, B.S. 2019. Case Study Research. In: Van den Bulck, H., Puppis, M., Donders, K. and Van Audenhove, L. eds *The Palgrave Handbook of Methods for Media Policy Research.* Cham: Palgrave Macmillan, pp. 71–84.

Mufamadi, S. 2018. High Level Review Panel on the State Security Agency. [Online]. [Accessed 27 May 2024]. Available from: https://www.gov.za/sites/default/files/gcis_document/201903/high-level-review-panel-state-security-agency.pdf.

News24. 2011. *'Secrecy bill' a step backwards*, 17 September. [Online]. [Accessed 9 May 2024]. Available from: https://www.news24.com/News24/Protection-of-Information-Bill-a-step-backwards-20110916.

Parliamentary Monitoring Group. 2008. Protection of Information Bill [B28-2008]: public hearings (minutes), 29 July. [Online]. [Accessed 9 May 2024]. Available from: https://pmg.org.za/committee-meeting/9394/.

Parliamentary Monitoring Group. 2010. Minister of State Security second meeting on concerns raised during public hearings (minutes), 21 October.

[Online]. [Accessed 10 May 2024]. Available from: https://pmg.org.za/committee-meeting/12172/.

Protection of Information Act 84 of 1982. [Online]. [Accessed 9 May 2024]. Available from: https://ictpolicyafrica.org/en/document/vai7gcookbi?page=1.

Protection of Information Bill B6-2010. [Online]. [Accessed 9 May 2024]. Available from: https://www.gov.za/sites/default/files/gcis_document/201409/b6-10.pdf.

Quintal, A. 2021. South African journalist Sam Sole on landmark court victory: '2008 surveillance was the tip of the iceberg' (blog). *Committee to Protect Journalists*. [Online]. [Accessed 13 May 2024]. Available from: https://cpj.org/2021/02/south-african-journalist-sam-sole-on-landmark-court-victory-2008-surveillance-was-the-tip-of-the-iceberg/.

Right2Know Campaign. U.d (1). About R2K. [Online]. [Accessed 16 May 2024]. Available from: https://www.r2k.org.za/about/.

Right2Know Campaign. U.d (2). Mission, vision and principles. [Online]. [Accessed 27 May 2024]. Available from: https://www.r2k.org.za/about/mission-vision-and-principles/.

Right2Know Campaign. 2010. *Founding statement*. [Online]. [Accessed 24 May 2024]. Available from: https://www.r2k.org.za/wp-content/uploads/2012/12/R2K_Founding_Statement-Let-the-truth-be-told-Stop-the-Secrecy-Bill.pdf.

Right2Know Campaign. 2013. Supporting organisations. [Online]. [Accessed 27 May 2024]. Available from: https://www.r2k.org.za/wp-content/uploads/R2K-Supporting-Orgs-july2013.doc.

Right2Know Campaign. 2016a. R2K welcomes the National Assembly's decision on Cecil Burgess (press statement). Polity, 16 March. [Online]. [Accessed 13 May 2024]. Available from: https://www.polity.org.za/article/r2k-r2k-welcomes-the-national-assemblys-decision-on-cecil-burgess-2016-03-16.

Right2Know Campaign. 2016b. *Big brother exposed – surveillance of activists*. Cape Town: Right2Know Campaign. [Online]. [Accessed 24 May 2024]. Available from: https://www.r2k.org.za/2015/04/28/publication-big-brother/.

Right2Know Campaign. 2018a. *Spooked: surveillance of journalists in SA*. Cape Town: Right2Know Campaign. [Online]. [Accessed 24 May 2024]. Available from: https://www.r2k.org.za/wp-content/uploads/R2K-Surveillance-of-Journalists-Report-2018-web.pdf.

Right2Know Campaign. 2018b. Second 2018 mid-term review (report).

[Online]. [Accessed 13 May 2024. Available from: https://www.r2k.org.za/wp-content/uploads/MTR2-2018-report.pdf.

Runciman, C. 2015. The decline of the Anti-Privatisation Forum in the midst of South Africa's 'rebellion of the poor'. *Current Sociology.* 63(7), pp. 969–71.

Satgar, V. and Williams, M. 2021. *Destroying Democracy: Neoliberal Capitalism and the Rise of Authoritarian Politics*. Johannesburg: Wits University Press.

Smith, D. 2012. South Africa's 'Secrecy Bill' attracts international condemnation. *The Guardian*, 13 June. [Online]. [Accessed 10 May 2024]. Available from: https://www.theguardian.com/world/2012/jun/13/south-africa-secrecy-bill-un-condemnation.

South African National Editors' Forum. 2020. SANEF welcomes the president's decision to review the 'Secrecy Bill' (press statement). [Online]. [Accessed 10 May 2024]. Available from: https://sanef.org.za/sanef-welcomes-the-presidents-decision-to-review-the-secrecy-bill/.

State Security Agency. 2017. Performance review: period 01 January–24 February 2017: CDSO Co-Workers 2016 Deployment Team attached to Braze (24 February 2017). [Online]. [Accessed 28 May 2024]. Available from: https://www.dailymaverick.co.za/article/2022-07-01-civil-society-organisations-release-boast-report-demand-accountability-for-rogue-spying/.

Thakur, C. 2021. Advocacy release: amaB wins battle against spying abuse as ConCourt declares bulk surveillance unlawful, Rica surveillance provisions unconstitutional (blog). [Online]. [Accessed 23 May 2023]. Available from: https://amabhungane.org/210202-release-amab-wins-battle-against-spying-abuse-as-concourt-declares-bulk-surveillance-unlawful-rica-surveillance-provisions-unconstitutional/.

Voice of America. 2010. South Africans organising against government secrecy Bill, October 2010. [Online]. [Accessed 10 May 2024]. Available from: https://www.voanews.com/a/south-africans-organizing-against-government-secrecy-bill-105874203/156515.html.

CHAPTER NINE

A civilian-driven model for surveillance oversight in Zimbabwe

Allen Munoriyarwa

Introduction

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

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

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

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

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

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

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

I draw on Patel's (2019) argument that surveillance overreach is supposed to be understood as a failure of agencies. In addition to this, I also draw on an argument I made earlier (see Munoriyarwa, 2022) that the politicisation and subsequent polarisation of surveillance agencies constitute failure. In so doing, I want to extend an argument that I make (see Munoriyarwa, 2022; and forthcoming – 2025), and many other scholars, (for example, Moorcraft, 2012; Chan, 2019), that the Central Intelligence Organisation (CIO), Zimbabwe's premier intelligence agency, has declined in terms of efficiency. It has become rotten from the inside and has become a political appendage of ZANU-PF, the ruling party, which uses it as an instrument to retain power, by haunting both internal and external opposition to those in power. Elsewhere, other scholars (see Moorcraft, 2012; Moyo, 2014 and Chan, 2019) have noted that the CIO has basically become part of the ruling party, ZANU-PF's apparatus of violence and civilian subordination. For example, Simpson and Hawkins (2018) note that in the 2008 general elections, the CIO saved Mugabe and ZANU-PF from a violent political meltdown by becoming a reactionary apparatus of the party, violently suppressing civilian-led protests against a debilitating economic crisis. Tendi (2016) notes that they were, furthermore, very much involved in the ZANU-PF succession disputes that led to the overthrow of Robert Mugabe in a military coup. All these assertions point to the failure of surveillance agencies. As Gill (2020) and Owen (2012) note, failures like the ones I have outlined here are a result of the failure of oversight. With proper oversight-function mechanisms, the CIO would not have engaged in such blatant and egregious mission creep practices. It means the existing model of oversight has not worked in Zimbabwe. What other oversight models can be practised in order to avoid such failures? Building on these arguments, I extend the debate by examining how, over time, intelligence institutions became weaponised, politicised and militarised. I further extend the debate by proposing what I call a multifaceted civilian-driven model that can remedy these excesses in semi-authoritarian contexts using Zimbabwe as a point of entry. By semi-authoritarian regimes, I draw on an earlier definition we used (see Munoriyarwa and Chibuwe, 2021). I mean regimes that maintain a facade of democracy but dissolve its substance. For example, they hold periodic elections, which are not free and fair; they set up oversight mechanisms of certain government functions but dissolve some others; they allow many newspapers, but dissolve media diversity. Furthermore, semi-authoritarian regimes politicise, manipulate and weaponise state institutions to maintain political power and hegemony. Semi-authoritarian regimes often weaponise state security agencies to maintain internal tranquillity within their own parties. In other words, state security agencies within these regimes can be used in a partisan manner to prop one faction of the ruling party against another.

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

Background

Zimbabwe is increasingly contending with a slew of digital surveillance practices ranging from location surveillance, public-space surveillance and many more (MPDP, 2019; MPDP, 2021). The CIO has been, historically, responsible for much of this surveillance on civilians (MPDP, 2019). As such, credible reports have noted that the agency has purchased different surveillance technologies from as far as China and Iran. For example, in 2012 there are reports (see *The Zimbabwean*, 2019) that the CIO purchased email-hacking technologies from Iran. There were also reports (see Hawkins, 2018) that the CIO had purchased some IMSI catchers from China. Government security ministries justify this range of practices by arguing that they are necessary as crime-fighting measures and protection of the country from powerful colonial forces. However, the uses of these technologies come against a background of three other developments (Munoriyarwa, 2022). These are (a) an insufficient understanding of their use by both the public and the institutions administering most of these technologies; (b) regulatory gaps that leave room for abuse; and (c) the weaponisation of surveillance practices that lend the practice to political rather than intelligence uses (Ndlela, 2019; 2020). There are no known civilian-inclusive conversations about surveillance governance in the country and, consequently, the practice operates in a black-box manner (Munoriyarwa, 2024). The Interception of Communication Act (2007) provides the CIO with powers to undertake surveillance. There are also constitutional protections for civilians, at least on paper. Regulatory measures that protect surveillance from being practised in intrusive and covert ways are available on paper but not practised. For example, sections 207 to 210 of the Zimbabwe Constitution protect individuals and legitimate political parties from unlawful surveillance. Furthermore, section 207(2) is clear that surveillance agencies are subject to parliamentary oversight. Yet, despite this, there are no mechanisms to hold these institutions to account. There are also no practical regulatory mechanisms that ensure the legality and transparency of surveillance. Sections 224 to 226 of the Constitution of Zimbabwe prohibit the CIO from engaging in party politics. In addition to this, Section 210 prohibits the military from engaging in party politics as well. However, in reality, this has not been the case. There are incidences of surveillance of activists that have been reported in Zimbabwe.[3] Even as far back as early 2000, Mugabe's

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

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

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

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

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

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

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

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

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

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

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

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

This chapter draws on two sets of data. Primarily, it draws on 16 in-depth interviews with several actors with an interest in state intelligence and surveillance regulation and oversight. These interviewees were drawn from members of the last National Assembly (NA) (some of whom remained in the 2023 parliament) from both the ruling party and the opposition (formerly known as the Citizens Coalition for Change, formerly led by Nelson Chamisa). There were precisely seven members of Zimbabwe's NA interviewed. Three were formerly of the ruling party, ZANU-PF, and four from the opposition. Three interviewees were lawyers, two were members of network service providers and two were civil society activists who work in the field of digital rights and privacy. Lastly, two were journalists. For anonymity, which was guaranteed, they will be coded as part of this analysis. Among other issues, the interviewers sought to ask the respondents: how did the politicisation of Zimbabwe's intelligence agencies happen? The interviewers also sought to understand the extent to which these agencies still serve national security; the effectiveness of the oversight mechanisms available; and what can be done to ensure oversight and accountability of intelligence agencies. These are some of the questions they were asked. These interviews will be augmented by document analysis, drawing on credible news reports, CSO reports and any other credible documents available. For data analysis, document analysis will be used, drawing on credible information drawn from the documents analysed. The interviews will be subjected to thematic analysis that draws out major themes from the interview data.

Oversight of Zimbabwe's security agencies

Zimbabwe's CIO, a civilian agency, is constituted in Section 207 of the country's 2013 Constitution. This section states that Zimbabwe has four primary security agencies: the Zimbabwe Defence Forces (ZDF), the police services (Zimbabwe Republic Police [ZRP]), the CIO and the Prisons and Correctional Services. However, in Section 207 (e), an Act of Parliament can provide for establishing other security services. It is important to note that the CIOs are part of the country's security establishment. Furthermore, it is important to note that the ZRP and ZDF have separate intelligence agencies. For example, the ZRP's internal intelligence agency is called the Police Internal Security and Intelligence (PISI). PISI is supposed to focus on internal police intelligence, while the ZDF's intelligence unit should focus on military-related intelligence. The prisons and correctional service have their own internal intelligence unit. The senior commanders of ZRP, ZDF, CIO and prisons all constitute the Zimbabwe National Security Council (NSC) in terms of Section 209 of the Constitution. The NSC, chaired by the president and including the two Vice Presidents, ministers and members of the security services, is responsible for strategic security planning and coordination. The Constitution of Zimbabwe provides for both executive and parliamentary oversight of the intelligence agencies. As stated earlier, section 209 provides for the NSC, which the president chairs. Section 210 is named 'Independent complaints mechanism' and it states, 'An Act of Parliament must provide an effective and independent mechanism for receiving and investigating complaints from members of the public about misconduct on the part of members of the security services and for remedying any harm caused by such misconduct.'

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

> A warrant (for surveillance) shall be issued by the Minister to an authorised person . . . if there are reasonable grounds for the Minister to believe that
>
> (a) Any of the following offences has been or is being or will probably be committed (i) a serious offence by an organised criminal group.
> (b) . . . the gathering of information concerning an actual threat to national security or to any compelling national economic interest is necessary.
> (c) The gathering of information concerning a potential threat to public safety or national security is necessary.

> In exercising the above, the minister and the CIO are governed by Section 208 of the Constitution, which provides for the conduct of the security services. Section 208 states that no security agent shall:
>
> (a) act in a partisan manner
> (b) further the interests of any political party
> (c) violate fundamental rights and freedoms
> (d) prejudice the lawful interests of any political party.

These constitutional clauses are further fortified by Section 208 (c), which is clear that no members of the security services shall be active office bearers of any political party and that no member of the security service shall be employed by the civilian institution(s). There are several points to note in these clauses. Section 210 provides for an independent complaint mechanism. Admittedly, this is oversight, but it does not go far enough to encompass issues like the CIO budget, their intelligence-gathering activities of the year, their capabilities and an assessment of the credibility of the threats they investigate. The section focuses on complaints specifically. In practice, this oversight does not even exist, even in attenuated form. This has allowed the CIO and other intelligence agencies to operate with impunity. Recent incidences demonstrate this impunity, which thrives as a consequence of this lack of oversight. On 29 December 2023, the PISI summoned the veteran journalist and Director of the Information for Development Trust (IDT), Tawanda Majoni, to Harare Central Police. The IDT is an investigative-journalism hub that supports the local and Southern African media and journalists in probing corruption, human-rights abuses and socio-economic violations relating mostly to the public sector. It was formed in 2015 and, since then, has helped scores of journalists produce more than a hundred investigative stories exposing malpractices in the public and private sectors.[8] The second incident involves the president, Emmerson Mnangagwa. On 10 November 2023, Mnangagwa announced that he had appointed the Commander of the ZDF, General Phillip Valerio Sibanda, to the ruling party's highest decision-making body, the politburo. This blatantly violated Section 208 (a and b) of the Constitution, as read with 208 (clauses 3 and 4). It was human-rights lawyer Kudzayi Kadzere who threatened to sue the president if he did not annul the appointment. There was no quest for explanation from any parliamentary oversight body after these two incidences. For example, General Sibanda was appointed on 10 November, and the appointment was subsequently annulled on 23 November. No parliamentarian in the two weeks that followed requested any explanation despite the egregious violation. This demonstrates lapdog oversight, or rather, its absence in a captured parliament. In addition to this, Section 6(1) gives powers to the Minister of State Security; there is a provision for parliamentary oversight and to determine warrants. On the other hand, the NSC, in terms of Section

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

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

Intelligence accountability and oversight in Africa

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

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

The works of Duncan (2018; 2022) constitute part of this emerging foundational literature. Broadly, Duncan (2018; 2022) makes the overarching argument that, without oversight, surveillance can be abused for political purposes. The abuse of the South African intelligence by former president Jacob Zuma is telling evidence of this possibility even in countries deemed to be democracies (Duncan, 2018). Without oversight, Duncan (2022) argues, there are several risks that can easily debilitate intelligence agencies, for example, as noted previously, their politicisation. However, there are further risks that include internal decline, corruption, power struggles and outright failure of intelligence (Duncan, 2022). Elsewhere in Africa, the Africa Defence Forum (ADF, 2023) has argued that the increasing growth of surveillance technologies across most African countries requires vigilance in oversight of end users – the intelligence agencies. The ADF argues that this immense growth of surveillance technologies empowers intelligence agencies, but requires corresponding powers of oversight (ADF, unpublished). Kuwali (2023) agrees with ADF, noting that intelligence and security agencies need oversight to ensure that they are subject to the law. Kuwali (2023) agrees with Duncan (2018; 2022) that weak oversight of intelligence agencies can inhibit professionalism. The parliament of South Africa (n.d.) has noted that oversight is critical for other aspects like control of surveillance practices, which stops rogue surveillance agencies from conducting unwarranted surveillance, accountability and budgetary control. The agreement in this literature is that there is a need for oversight and accountability to avoid intelligence overreach and excesses like the targeting of legitimate political opponents, activists, communities and journalists. There is also a need, as the available literature suggests, to institute oversight of the intelligence institutions to guard against internal turmoil, politicisation, corruption and rogue intelligence agencies. Much of the literature on surveillance oversight in Africa is still in policy briefs, rather than academic empirical research (see, for example, Hutton, 2009; Kuwali, 2023) and newspaper briefs (see, for example, ADF, 2023). Duncan's (2018; 2022) remains the most recent intellectual work on intelligence oversight on the continent. This points to the existence of a huge gap in the need for more empirical research on the subject. Southern African researchers, particularly in Zimbabwe, Mozambique, Zambia and Malawi, have not mustered much research on intelligence oversight. This chapter attempts to fill this gap by examining possible routes of intelligence oversight in a Zimbabwean context.

Understanding oversight as a practice

The debate on oversight often takes different dimensions, depending on the context. In Africa, for example, where the demand for oversight of the intelligence agencies is still emerging, policymakers and activists are still grappling with the question of why, in the first place, oversight of the intelligence agencies is needed (Hutton, 2009) and, related to this question is its historical origin (Wegge, 2017). In advanced democracies these questions are fairly settled. The debates are now around what kind of oversight and what it can do to intelligence agencies. Intelligence oversight is part of a process that ensures some form of both transparency and accountability for intelligence services (Glees, 2011; Patel, 2019). Generally, there are two types of mistakes intelligence agencies can make (Brown, 2011) that require oversight. The first one is the failure to detect threats in advance (Brown, 2011; Goldman and Rascoff, 2016). The Pearl Harbor attack,[9] the 9/11 and the London bombings of 7 July 2005 are examples of how intelligence agencies can fail, and how oversight can hold them to account, and flag internal weaknesses that can lead to these failures. Such a failure is a consequence of several factors, including, chiefly, the collection of wrong information, erroneous assessments of intelligence information, inaccurate information and a lack of adequate resources (Brown, 2011). The second level of failure that requires oversight is abuse of power (Goldman and Rascoff, 2016; Mare and Munoriyarwa, 2026). Oversight ensures that intelligence agencies do not infringe on civil liberties and human rights in the name of national security (Brown, 2011). Oversight is useful to flag down aggressive protection of citizens that does not adhere to laws, including indiscriminate collection of data for mass surveillance. Intelligence oversight, therefore, is not only about setting the rules for intelligence agencies. It is about whether the rules have been complied with and whether they are providing an outcome that was intended of them (Brown, 2011; Kamarck, 2021). In the era of technology, oversight is meant to ensure that surveillance agencies are using technologies properly and not using these technologies to thwart legitimate political activities or to gather intelligence that may lead to the torture and harassment of citizens. Beyond these two issues, oversight is also necessary to check the unnecessary expansion of intelligence agencies, which might lead to an ever-growing burden on the fiscus (Brown, 2011). More so, oversight is a form of check on the politicisation and capture of intelligence agencies by ruling regimes.

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

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

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

Findings

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

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

Firstly, how did the state intelligence agencies, especially the CIO, mutate into violent party-aligned intelligence agencies? To understand the contemporary capture of Zimbabwe's intelligence agencies, one needs to understand the history of intelligence agencies themselves, in colonial Zimbabwe. (The country was referred to as Rhodesia before independence.) A close look at the country's intelligence agencies would show that the postcolonial intelligence agencies, military intelligence and the CIO are two sides of the same coin. The main purpose of intelligence agencies is the preservation of national security. National security is a valence issue – an ideal shared by all political players. However, in colonial periods in Zimbabwe the CIO's role went beyond this. While the intentions of setting it up were to preserve national security by pre-empting attacks through intelligence gathering, the CIO became a political appendage of the Rhodesian Front (RF), the ruling party of the colonial era. Ken Flower established the CIO under the colonial Prime Minister Winston Field (Megahey, 1998), although the discussion to set up an agency had started long before under the Prime Minister Edgar Whitehead. Even though Ken Flower always saw himself as apolitical (Preston, 2004), his activities became very much political. For example, his alleged direct involvement in setting up a militant movement (RENAMO) to counter FRELIMO in Mozambique (Alao 2012). Thus, from its formation, the CIO meddled in politics and became part of the institutional mechanisms on which the RF drew its political powers to manage increasingly restive and militant colonised Black populations in the country (Matthews, 1999). The idea was to weaken and destabilise Mozambique's role as a host of Zimbabwe's guerrilla movement but, in addition to this, to save the RF as a ruling party as well. Thus, while the colonial CIO's role can still be located within the realm of security intelligence, its politicisation was rooted in its formation in 1963. It was also, furthermore, manned by RF sympathisers of varying commitments.

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

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

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

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

The process of politicising the intelligence agencies was not only driven by Mugabe's relentless pursuit of total power, but by his enablers in both the government and security services. Chief amongst these enablers included ministers and military commanders. For example, researchers Burke (2018) and Matyszak (2018) note that Emmerson Mnangagwa, the current president, was the 'go-to fix it' person (n.p.) for Mugabe. These are the people, within the ruling party, who pushed Mugabe's project to capture and 'Zanufy' state institutions like intelligence services. A report[10] on intelligence notes that with the help of his numerous enablers, Mugabe weeded out perceived internal opponents in the CIO. These include elements of the Zimbabwe People's Revolutionary Army (ZIPRA), a guerrilla movement led by nationalist Joshua Nkomo, that had also fought, alongside ZANU-PF, for the liberation of Zimbabwe. The report notes thus:

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

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

Factionalism in the ruling party and state intelligence capture

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Pathways to oversight of intelligence

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

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

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

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

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

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

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

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

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

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

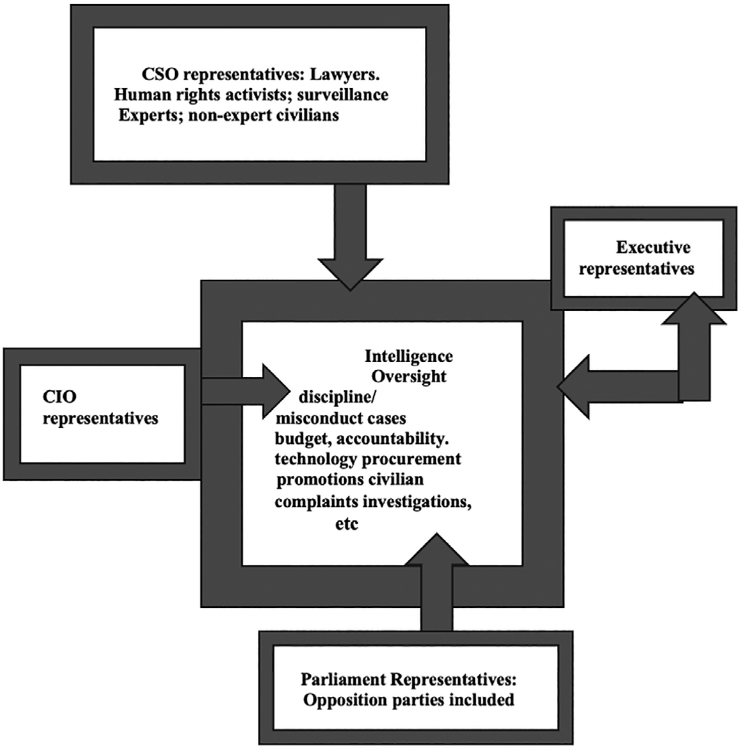
CSO representatives: Lawyers.
Human rights activists; surveillance
Experts; non-expert civilians
Executive
representatives
CIO
representatives
Intelligence
Oversight
discipline/
misconduct cases
budget, accountability.
technology procurement
promotions civilian
complaints investigations,
etc
Parliament Representatives:
Opposition parties included

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

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

Discussion and conclusion

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

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

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

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

This sums up what can militate against civilian inclusion. There will be obvious resistance from the CIOs themselves and the Executive. But if parliament is not willing to act, then the whole idea of civilian oversight will be difficult to implement. Added to these factors are three other important issues about the Zimbabwean political context. The first issue is ZANU-PF's exaggerated sense of self-entitlement to the Zimbabwean polity will likely work against anything that brings civilians on board. Added to this is the polarised nature of Zimbabwe's politics that makes it difficult for parties to find common ground and engage in logrolling practices during lawmaking debates. Lastly, trust and suspicion in the polity are still rife. Future research should, perhaps, focus on how civilian trust and awareness about intelligence agencies can be built in order to involve them in intelligence oversight structures.

References

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

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

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

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

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

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

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

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

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

Glees, A. (2011). European Security Intelligence. In Jorgensen, K. E., Laatikainen, K., Drieskens, E., & Kalland Aarstad, A. The SAGE handbook of European foreign policy Volume Two, (pp. 264-276). London: SAGE Publications Ltd.

Hawkins, A. 2018. Beijing's Big Brother tech needs African faces: Zimbabwe is signing up for China's surveillance state, but its citizens will pay the price. *Foreign Policy*. [Online]. [Accessed 13 August 2020]. Available from: https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CHAPTER TEN

Current trajectories and future challenges for public oversight

Jane Duncan and Allen Munoriyarwa

Introduction

In this concluding chapter, we assess the major findings from each of the chapters and return to the original question posed in the introduction, of how the public can perform more effective oversight digital surveillance for intelligence purposes. Each chapter has presented case studies of moments when public oversight has been attempted and either succeeded or failed or achieved mixed outcomes. All the cases discussed could be considered examples of public oversight, or the superintendence of intelligence in a manner that is independent from the everyday management and practices of intelligence and the institutions that collect, analyse and store it, to ensure accountability. They detailed examples of the public engaging in demands for radical transparency in this secretive area of state power, by exercising 'watchful care' over how digital surveillance has been used and abused. The chapters analysed moments when the public required intelligence agencies to explain and justify surveillance and change surveillance practices when they amounted to abuse (McCarthy and Fluck, 2016). Some of these cases involved intelligence and surveillance laws or state-sanctioned data-processing systems that the public feared had surveillant potential. Others followed the shock-driven approach to intelligence reform, where controversies around surveillance abuses came into the public domain through whistleblowing or the leaking of intelligence information, and these controversies galvanised public action of various kinds (Johnson, 2018, p. 209–46). This chapter uses a summary of the main chapter findings to address key research questions and to develop a set of theoretical propositions about public oversight and the conditions under which it is likely to succeed.

The case studies: Main findings

The Angolan case examined an example of successful public oversight, namely the highly controversial 15+2 case where activists were released followed by a general amnesty after an international campaign following their conviction for organising a reading group the then government considered to be threatening. The 15+2 case saw public oversight compensating for weaknesses in the security services and the courts, both of which were shown to lack independence from the ruling party, resulting in the hasty approval by parliament of an amnesty law after a massive international outcry over the convictions of the accused. The fact that Angola is what the author characterised as an anocratic regime, which is inherently unstable, made it more susceptible to public pressure as its political institutions were weak, the rule of law was applied inconsistently and the government lacked the capacity to maintain central authority and manage conflict effectively. The case study suggested that far from being adept at coercive control, the security services were poorly institutionalised and vulnerable to marginalisation within government when their ineptness became politically embarrassing.

However, the case was marked by a disjuncture between the success around the 15+2 case and the actual capacity on the ground to perform public oversight in Angola. The success of the campaign could not be sustained and deepened into a lasting movement that changed the oppressive state-society relations that continue to beleaguer Angolan society. The public oversight that was performed was very truncated and scandal-driven, focusing particularly on the hunger strike of Luaty Beirão and the embarrassment it caused the government. The government was responsive mainly to international organisations and adverse publicity in the Portuguese press and the US diplomatic establishment, rather than local pressure. This outsized focus on international outrage suggested a lingering deference to its former colonial power and the US, and a reluctance to take local actors seriously. Consequently, once all the international fanfare around the case had died down, it became apparent that there had been no lasting changes in oversight practices and even journalists, as potentially a more well-organised and resourced social force, were ill-equipped to take on the challenge.

Botswana is widely considered to be on the democratic end of the political spectrum, yet this characterisation masks deeper authoritarian tendencies that manifest themselves in centralised control of civilian intelligence. The author attributes these authoritarian tendencies to a continuity of intelligence and surveillance practices from the colonial-era police Special Branch with its political intelligence-gathering mandate in the furtherance of empire and deliberate lack of oversight, to the democracy-era DIS and notwithstanding the fact that the DIS was a postcolonial creation. The author also pointed to the lack of professionalisation of intelligence, evident from its factionalisation, where different factions of the ruling party misused surveillance capabilities to keep one another under surveillance. The courts provided some respite in performing more independent official oversight and have shown that they would not be deferential to the executive on national-security matters (a term which remains ill-defined). However, the centralisation of the DIS under the presidency undermines accountability, as it gives the president the secretive powers of intelligence to settle scores. Oversight has been introduced begrudgingly and limited in various ways.

Nevertheless, there exists some national capacity for public oversight in Botswana and, as was shown in the campaign around the Criminal Procedures and Evidence Bill, established human-rights and media organisations can collaborate on surveillance overreach when they need to do so, to the point of lobbying parliament effectively on a bipartisan basis before the debate on the Bill. The campaign against the Bill also received strong regional and international support, particularly through the organised media, and especially from editors. The government was open to changes to the Bill, but not to the extent of including a provision around post-surveillance notification, where surveillance targets are informed that surveillance had occurred once the case reaches a non-sensitive stage. The campaign was also boosted by journalists who had access to whistleblowers within DIS, who tipped them off that they were under surveillance, providing some evidence of abuses and taking surveillance out of the realm of an abstract possibility and into the realm of a real and pressing threat to media freedom. However, the difficulty of obtaining funding for sustained public oversight has proved to be an obstacle, as is the lack of resources for investigative journalism and the lack of independence of civil society organisations and journalists. The lack of accountability of the media also limits their ability to act as credible watchdogs over the intelligence sector.

The DRC provides interesting and instructive examples of public oversight and a possible way forward in terms of how to organise it, in ways that legislate cooperation by all the main actors in relation to surveillance and its oversight. In the case of the campaign around the controversial Registry of Mobile Devices, or RAM, public pressure led to an unpopular RAM tax being abolished, which the author analysed in terms of the theory of affected interests, where action is more likely to be taken by a political community when common interests are affected by a national decision. In contrast, other surveillance cases in the DRC did not lend themselves to mobilisation as the issues were more abstract and individuals were affected. However, in at least one case, where a journalist, Stanislas Bujakera, was convicted for sharing what was alleged to be false information from the internal-security department of the National Intelligence Agency, and on the dubious grounds that the information came from his Internet Protocol (IP) address, public pressure was also brought to bear on the case to the extent that he was released despite having been convicted. In a striking similarity to the Angolan case, the foreign media had a strong role to play in this case, particularly the French press, suggesting that the government was sensitive to foreign criticism. Yet, despite the successes of these two cases, surveillance oversight has not become a specialism of civil society in the DRC, although there was potential for this to happen given the legislating into being of local-community safety councils with the responsibility to develop local-community safety plans, and the potential to include representatives of public authorities and civil society organisations. These councils could provide the basis for sustained, bottom-up oversight of security powers, including surveillance. However, as legislated bodies they remain vulnerable to political control, evident from the fact that they still require a presidential decree to bring them into being.

Like Botswana, Namibia is an example of a stronger democracy than most in the region, with a highly centralised civilian-intelligence agency but with capacity in civil society to perform sustained and informed public oversight, despite the country's small population. Unlike Angola, Namibian civil society has been able to achieve a more consistent and less scandal-driven form of oversight. The NCIS has poor internal controls and external oversight, but in the case of *The Patriot* newspaper, the judiciary stepped in and asserted its right to perform oversight, which the NCIS accepted, suggesting respect for the rule of law. Namibia has strong domestic civil society capacity to deal with the technical issues around surveillance and to translate them into publicly understandable messages, a case in point being SIM-card registration and its surveillant potential, through consistent civil society and media work on the issues, leading to the media and civil society contributing what the authors have referred to as a democratic subsidy around intelligence oversight. International actors have played a consistent monitoring role and, to that extent, their interventions have been less episodic and scandal-driven than in Angola. Opposition politicians also raise important issues around surveillance, which brings the electoral competition that does exist to bear on the problem. However, even though capacity does exist, public oversight can be, and has been, overridden on key issues, showing that it still lacks the social power needed to act as a brake on surveillance abuses or initiatives with surveillant potential.

Mauritius is a compelling example of a successful case of public oversight and the chapter was one of several that pointed to the diversity of surveillance practices or state practices with surveillant potential. This diversity complicates oversight as it requires anti-surveillance activists to do more work than they ordinarily would need to, to explain why the public should be concerned. In this regard, the author examined the potential for a centralised, smart, biometrically based ID card to become a tool for digital surveillance, and used a mixed-theory approach to examine the factors that allowed the campaign against the smart-ID-card system to achieve at least partial victory. She concluded that organised political forces or policy entrepreneurs in Mauritius exhibited a high degree of consensus that led to successful public oversight, and a change in government also played a role in the amendment of the biometric ID card. Their mobilisation strategies included being able to frame a government initiative to improve citizen-identification services that would, on the surface of things, have little to do with intelligence-led surveillance, as one with surveillant potential and a potential danger to citizen privacy. They were also able to mobilise a broad cross-section of society through popular campaigns that extended to the political opposition who took the campaign up as part of an electoral platform. The author attributed successful mobilisation to a combination of specific historical factors, notably the international context of heightened sensitivity to the dangers of surveillance that co-incided with the Snowden revelations, as well as public sensitivity to the potential for government surveillance before an election. There were also deeper factors peculiar to Mauritius as a society that contributed to this success story, such as a deep concern for privacy and enmity towards government initiatives that smacked of surveillant colonial practices, a mobilised and deep-rooted culture of organising and political opportunities to ensure that activism had an effect, although there is more recent evidence of democratic backsliding. There is much to be learnt from how the campaign against the smart-ID-card system was organised, as these lessons can be applied elsewhere in the hope of achieving similar successes. However, the structural conditions that made Mauritius receptive to the activism were peculiar to Mauritius and were unlikely to be replicated in other countries with different histories and social structures.

Mozambique presents a much bleaker picture, in that it showed deep continuity between Portuguese colonial and postcolonial intelligence practices, and the fact that Mozambique fuses democratic and authoritarian characteristics facilitated this continuity. The Portuguese International State Defence Police were involved in the maintenance of colonial rule until the popular uprising in Portugal itself, but this colonial tradition of using intelligence for political policing was embraced by Frelimo, and they used the civil war as a pretext to maintain these problematic surveillance practices. They also militarised state intelligence under the party's control, initially through a one-party system, and then through a nominally democratic political system with the appearance of electoral competition and institutionalised, professionalised intelligence services, but with very little substantial democratic content. This lack of a democratic culture accounts for the failures of civil society to mobilise successfully against the government's centralised, expansive intelligence and surveillance powers, as government has promoted an uncritical citizenry. The government has made the abuse of these powers more likely by keeping the legal remit and accountability of postcolonial intelligence deliberately unclear, and collapsing the separation of powers between the executive, legislature and judiciary on the basis that it has the moral authority to lead all aspects of society.

South Africa, on the other hand, offers a mixed picture of tremendous success in activist mobilisation and strategic litigation against state secrecy and the excessive power of state intelligence services under former president Jacob Zuma, followed by an inability to sustain a campaigning style for public oversight. The author examined how an attempt to establish a popular campaign that attempted to combine the best traditions of non-governmental organizations (NGOs) and social movement organising led to a campaign that broadened out from a focus on a Protection of State Information Bill to include intelligence and surveillance abuses that appeared to be taking place under the guise of intelligence secrecy. The campaign was able to generalise intelligence and surveillance abuses across society by relating them to popular struggles against exploitation and oppression, thereby making them relevant to affected interests. The lack of definition of the campaign's popular base proved to be the campaign's undoing, though, with anti-surveillance work having to shift gear and focus on strategic litigation and culminating in a blockbuster victory against South Africa's main surveillance law, Rica, in the Constitutional Court. However, strategic litigation lacked a popular base and was unable to maintain public pressure after the Constitutional Court case. Ultimately, anti-surveillance activism in South Africa was a victim of broader demobilisation of social movements in the wake of the 2008 global recession and underscored the need to use litigation without sacrificing a popular base and social-justice focus.

In the case of the semi-authoritarian Zimbabwe, intelligence services have been highly partisan from the colonial and pre-independence periods, with no real period of professionalisation after independence. The author examined how the first post-independence leader, President Robert Mugabe, set about designing Zimbabwe along deliberately authoritarian lines. The civilian intelligence agency, the CIO, which was absorbed wholesale into the government from the colonial era and which was responsible for the maintenance of British imperial interests in then-Rhodesia, followed by white minority interests, was central to his designs. This longstanding problem of intelligence partisanship has led to mission creep, where the country's military intelligence where the country's military intelligence have meddled in civilian matters, as the CIO could not be trusted even within the ruling ZANU-PF government due to its alignment with Mugabe. ZANU-PF became factionalised, which ironically, created greater potential for activism around surveillance abuses as these concerns reached right up to the highest levels of the political establishment as different factions feared being spied on by other factions. Nevertheless, there was no real public outcry when prominent Zimbabweans were put under surveillance, echoing the finding of the DRC chapter about the lack of affected interests. However, the fact that intelligence services in Zimbabwe have discredited themselves through partisanship, especially the CIO, has created scope for reform, as has the limited scope for parliamentary and judicial oversight given the lack of independence of these institutions. In view of these challenges, the author proposes a multivariate model of oversight that involves the key actors into an institutional mechanism that locks the official actors into a civilian-led oversight mechanism, rather than relying on them to perform oversight of their own initiative, and forces greater transparency and accountability in how state intelligence conducts surveillance.

Bringing the findings together: Assessing the state of public oversight

The chapter findings provided data to attempt answers to the research questions posed in the introduction. The Angolan 15+2 case, the Botswana campaign around the Criminal Procedures and Evidence Bill, the campaigns in the DRC against the RAM tax and the release of journalist Stanislas Bujakera despite his conviction, the campaign against the smart-ID-card system in Mauritius, the case involving reportage by *The Patriot* newspaper on corruption in the Namibian NCIS's and the Agency's failed attempt to prevent publication, and the anti-surveillance and anti-secrecy campaigning, culminating in strategic litigation against Rica in South Africa, are some of the stand-out moments discussed in the chapters. They were examples of successful public oversight, in that these democratic victories against extant or potential digital surveillance abuses extracted costs from the respective governments and were won through public action. The Botswana and South African cases had lasting impact in that laws were changed in ways that reduced the scope for surveillance abuses beyond the scandals that brought the issues to public attention. Actions taken ranged from strategic litigation to lobbying of policymakers and legislators, public education, pickets and protests, investigative journalism and media publicity. The indicators of success were that these public oversight interventions led to individuals who had been convicted wrongly, being released or not being imprisoned, the abandonment or partial abandonment of government initiatives with surveillance potential and the redrafting of laws allowing for surveillance overreach.

All these countries had differing opportunities for formal oversight, with South Africa offering the most opportunities. Nevertheless, the formal oversight mechanism barely features in the successful case studies as having contributed to meaningful oversight, except for the judiciary. Interventions were more likely to succeed when public interventions could appeal to a responsive court system willing to act independently from the government on national security matters, when intelligence agencies respected court decisions, when campaigns had an international element, and when established civil society actors adopted a popular campaigning element combined with technical expertise on digital surveillance. Journalists and journalists' organisations could also play a decisive role with their ability to mobilise resources, provide publicity and explain the dangers of digital surveillance to the public.

The ineffectiveness of formal oversight institutions provided opportunities for public oversight. During economic downturns, voters tend to withdraw from the electoral system, and this trend is pronounced across Africa (Halfdan and Coma, 2022). The decline in electoral participation has implications for formal oversight, especially parliamentary oversight, as it can lead to a loss of confidence in electoral politics that provide state institutions with the legitimacy to perform oversight on behalf of the public. If more governments are governing with smaller voter mandates, then the edifice on which state institutions, including intelligence oversight institutions, is built becomes fragile indeed and open to question. On the other hand, the citizenry, including disaffected non-voters, could become activated for public oversight, allowing for deeper citizen participation in how intelligence agencies are held to account.

There is evidence of capacity to sustain oversight having been built to different extents in Namibia, Mauritius, Botswana and South Africa, and this capacity includes the technical knowledge needed to engage with official actors on what may be technically complex laws, policies and practices. This capacity is domestically based, with much of it being based in sectors of society that are relatively resource rich, such as NGOs, churches, investigative journalism organisations and editors' associations. South Africa and Mauritius also have traditions of popular organising and mass movements, and remain, relatively speaking, highly mobilised societies, and these traditions of organising provided a social base for anti-surveillance activism. The Mauritian, DRC and South African cases contained more elements of popular campaigns with broader social bases, but these have proved to be the most difficult to sustain given the resource poor nature of many of the social groups engaged in these campaigns and the difficulties of sustaining social movements in this historical period. These challenges are important to grapple with, as these broad-based campaigns have proved to be highly successful in performing public oversight as they can exercise considerable social power and cannot be marginalised easily.

With regards to failed public oversight, responses to mass surveillance and SIM-card registration in Mozambique and the surveillance of some prominent individuals in Zimbabwe and DRC, and the failure to prevent enactment of part six of the Communications Act in Namibia that provides for the monitoring of communications and SIM-card registration, are some of the standout failures. However, the Namibian government took many years to enact the relevant section, suggesting that they were sensitive to criticism, but not enough to stop the enactment.

The most difficult environments for effective public oversight are Mozambique and Zimbabwe, where no real breakthroughs in reining in digital surveillance abuses, are evident. While many countries show signs of continuities between colonial era surveillance practices involving political policing of the then-liberation movements, continuities are particularly pronounced in these countries. In the case of Zimbabwe, the CIO was literally a colonial invention and was absorbed into the post-independence presidency as is, rather than being shut down and a new intelligence agency being established in its place. As a result, it is hardly surprising that surveillance of dissent remains central to what the CIO does, as that is what it was set up to do. Mozambique's situation is slightly more complicated as it is more difficult to draw straight lines between colonial and post-colonial surveillance practices as the SNASP and SISE were post-colonial institutions. However, post-colonial Mozambique did adopt the lack of intelligence oversight, coupled with excessive centralised control and political policing of dissent, from the colonial Portuguese regime. The ruling parties of these countries also exercise strong control over the levers of society, making it extremely difficult for the public to organise effectively.

In contrast, Angola, which shares a similar colonial history to Mozambique's, is much more unstable, and the ruling MPLA's grip on society is weaker, creating space for more contestation around digital surveillance.

Mozambique faces the added problem of a culture of uncritical citizenship. While this problem is particularly pronounced in Mozambique, it is a problem shared by countries where former liberation movements became governing parties, as they face the risk of these parties overtrading on their liberation credentials, claiming to be the sole and authentic custodians of transformation values and limiting dissenting voices on the basis that they are counter-revolutionary. The fact that Mozambique had transitioned through a civil war and was battling instability in the Cabo Delgado region, also led to a lingering culture of fear coupled with a militarisation of civil functions, including intelligence. The government had little difficulty in justifying this militarisation on the basis that the country could lapse back into full-blown civil war if security institutions failed to maintain heightened vigilance.

With regards to public oversight with mixed outcomes, even the successful cases were episodic, ultimately leading to mixed outcomes in the longer term, where the pressure for reform subsided somewhat once the surveillance scandal died down. Namibian civil society has developed capacity to sustain work on surveillance oversight, but it is difficult to see what significant and lasting democratic gains have been made beyond the legal precedent set by *The Patriot* case. The disintegration of anti-surveillance activism in South Africa meant that the legal victory achieved through the Constitutional Court case was tempered somewhat by a Parliament and government intent on adopting the most conservative interpretation of the judgement possible. International NGOs and the international media have also emerged as strategic and, in some cases, problematic, oversight actors. The Botswana, DRC and Angolan governments have been sensitive to international criticism, and these cases raise complicated questions about who governments take seriously as oversight actors. However, in the case of the international NGO interventions, there is no evidence of them engaging in local capacity building, and it is at the domestic level where public oversight is likely to be sustained. As a result, once the scandal dies down and they turn their attention elsewhere, local organisations still lack the capacity to continue the oversight (Angola being a case in point). If lasting impacts on oversight are going to be achieved, then international NGOs need to change how they work on surveillance abuses in Southern African countries.

As the case studies show, the domestic capacity needed to sustain public oversight includes the policy capacity needed to understand and engage in areas that may be technically complex: the surveillance potential of Mauritius's smart-ID-card system, Namibia's SIM-card registration or DRC's IMEI registration, for example, require technical knowledge to explain. However, technical knowledge on its own is unlikely to be enough to convince policymakers to depart from unhealthy digital surveillance practices: activists would also need to bring public pressure to bear through direct actions within the confines of what is possible within countries where there are significant democratic limitations. These actions may include organising, public education and meetings, lobbying, picketing and pamphleteering, protests and strikes, to ensure that their arguments are taken seriously. Organising on a more popular basis could avoid the kind of statis that is evident in Angola, but without falling into the trap of over-inclusivity that South African anti-surveillance activists fell into.

It has also proved to be difficult to take up surveillance cases involving individuals, as activists face the challenge of reframing an individual injustice as a collective injustice. This has been easier to achieve in the case of journalists, who can be framed as 'worthy victims' whose surveillance cannot be justified and is likely to indicate a broader attack on media freedom and society's right to know. Surveillance of politicians, on the other hand, such as the ones subjected to surveillance in Zimbabwe, may be more difficult to frame as an injustice in situations where there are already low levels of trust in political institutions and the integrity of politicians. Despite the central role of the media in performing public oversight, as the Botswana case showed, media professionalisation, or the lack of it, can be a significant brake on its ability to perform public oversight that enjoys widespread legitimacy. Media systems may not be structured in ways that enable public oversight, particularly those with large state and weak private and community ownership and control (Zimbabwe being a case in point). As the Angolan 15+2 case has shown, social media can become an alternative outlet. One possibility is for journalists to collaborate internationally and, in this regard, global collaborative investigative journalism has become a major factor in the media being able to perform successful public oversight by exposing surveillance abuses. This form of journalism is allowing the burden of interpreting leaked documents to be shared across various newsrooms and has spread the risks of official reprisals across various media actors.

Some elements of effective oversight

So, what makes for effective oversight of intelligence-driven surveillance? There are no easy answers to this question, considering what the different chapters in this book, which delve into specific cases of oversight in various contexts, raise. Each chapter raised its own concerns, and every context raises its opportunities and challenges (Van Brakel, 2021). It is also difficult to anticipate changes – especially political – that are likely to take place and that may have a bearing on oversight. For example, changes in surveillance laws often affect how oversight will likely evolve in the future. In some contexts, these changes arise out of legislative initiatives, highlighting the need for constant vigilance and adaptability in the oversight process. An elected parliament may pass a law that (partially) overhauls surveillance and impacts on oversight. In other contexts, surveillance oversight may be midwifed by judicial pronouncements. For example, a higher court may strike down certain surveillance provisions, like what happened in South Africa in 2019 and 2021 (see Duncan in this book), and, in the process, overhaul surveillance oversight practices.

All of the above are realistic possibilities that militate against a one-size-fits-all approach to oversight. Furthermore, the countries researched are different politically. South Africa and Botswana have a tradition of constitutionalism. The same cannot be said about Zimbabwe, however, which actually has a reasonably strong constitutional basis for democratic oversight. Nevertheless, the country has drifted into a hardened authoritarian regime that maintains a façade of democracy (for example, through periodic elections) but dissolves the substance (for example, through prohibiting free and fair elections and maintaining captured and coercive state apparatuses). In the other countries discussed, there is less appreciation of inclusive institution-making. Thus, it is very difficult to say what an effective oversight model would look like. Two issues of agreement are, however, important to highlight. The first one is that every model currently known – judicial, legislative and executive – has strengths and weaknesses. For example, the judicial model may provide independent oversight (McIntyre, 2016), but it can be slow, cumbersome and costly. It can also be captured in (semi-)authoritarian regimes, as Munoriyarwa has demonstrated in this book. Conversely, the executive model may be more agile, but it can be prone to political influence. But, in all the cases we have examined here, there is very little evidence that any of them are working consistently, especially legislative and executive oversight. Increasing both transparency and accountability are the broader objectives of oversight (Butler, 2013; Newell, 2014).

However, public oversight is not guaranteed to be effective in detecting and preventing surveillance abuse, either. The cases we have documented in this book, for example, the DRC Heri Kalemaza case, show that while public oversight can detect arbitrary behaviour and illegal and unconstitutional conduct by surveillance agencies and speak back to these agencies' unfettered powers wherever they are exercised, it can still fail. When exercised, public oversight can still name and shame individuals within institutions who abuse surveillance powers. Where it has been attempted, as in some cases in this book, the objectives of public oversight, while clear, have been narrowly defined. The core objectives of public oversight have been protecting individual and citizens' rights and liberties (Murray et al. 2020) from arbitrary surveillance that lacks transparency and accountability and to protect human rights (Malgieri and De Hert, 2017). Broadly speaking, it means public oversight has consistently attempted to guard against state and surveillance agencies' excesses and hold them accountable for their powers.

Public oversight objectives can and should go beyond these narrow confines, though. Following the South African approach, the objectives of public surveillance oversight can expand (see Duncan's chapter). In South Africa, attempts at public oversight have been more holistic than in other countries whose experiences are chronicled in this book. They have included oversight over intelligence budgets and its (ab)use. Except for the South African case, the several cases that form this book do not often include this kind of oversight. Yet, it can be argued that surveillance agencies can only be as powerful (as well as abusive) as their budget permits them to be. Thus, whatever public oversight might end up being, one of the objectives should include ensuring that surveillance institutions do not waste taxpayers' money and operate functional machinery that serves the public interest within a stipulated budget. The South African and Zimbabwean cases in this book remain stark examples of why the fiduciary oversight responsibility is pertinent to any existing forms of public oversight envisaged. In South Africa, the State SSA agency budget was looted by highly (politically) connected individuals. It became a self-enrichment 'cookie jar' by organised criminal networks that had invaded and paralysed the agency and rogue SSA officials.[1] In Zimbabwe, the CIO budget had on several occasions been reported to be looted[2] by highly (politically connected individuals. The agency had been used to sustain a 'jobs-for-pals' culture where ZANU-PF officials' relatives are hired. Yet, in the cases constituting this book, there is very little evidence that attempts at public oversight in the different countries, except South Africa, have prioritised financial oversight within these intelligence agencies. This mechanism should protect rights and monitor the financial health of intelligence agencies, which is necessary for these agencies' long-term survival and integrity. We underscore the urgency and importance of a holistic public oversight mechanism

[1] More details can be found here: https://www.news24.com/news24/investigations/ssa-declassified-i-networks-which-looted-r15bn-from-spy-agency-still-in-place-as-investigations-collapse-20220221.

[2] The Zimbabwe case has been investigated and documented here: https://thenewshawks.com/financial-looting-exposed-at-cio/.

that not only protects rights but also monitors the financial health of intelligence agencies, which is necessary for these agencies' long-term survival and integrity.

As we have traced in its different forms of practice in this book, public oversight is a very complicated and ambiguous phenomenon. The term 'oversight' itself means looking over. It does not mean 'touching' as an example (being involved in the day-to-day management of intelligence agencies). By merely 'looking over', there are limited objectives that oversight can achieve. Some may not be easily achieved by 'looking over'. This does not mean to devalue it. It is merely highlighting its potential pitfalls as an alternative to formal intelligence oversight, which may be able to compel remedial action when abuses occur. This raises the second question: what kind of oversight can achieve most of the ideals – protection of individual liberties and privacy, financial oversight of state security agencies, transparency, accountability, as well contributing to more just and equal societies - without being involved in the day-to-day management of intelligence institutions, or without the level of involvement that can easily lead to accusations of interference? This is a very difficult question considering the disparate cases, scenarios, contexts and circumstances of each case study in this book.

Unpacking the key terms in public oversight of intelligence-driven surveillance

In order to move towards identifying a set of theoretical propositions about public oversight and the conditions under which it is likely to succeed, it is necessary to break the terms down into its different concepts, using the insights provided by the chapters, and then move onto the optimal combination of these concepts to achieve effective oversight.

PUBLIC

The different cases in this book show that defining the public is difficult, but there are a few points of convergence. The cases show that the public is not a neutral and democratic space that everyone has equal access to. It is a space for deliberation and action that is shaped by the deep inequalities persisting in the countries under discussion, leading to a fractured public sphere into multiple publics or even counterpublics (Fraser, 1992, pp. 109–42), which complicates the formation of the publics available to perform oversight. What is clear from the chapters, though, is that publics in the respective countries are constituted by outsiders to the intelligence community and, if there is a sufficiently clear common interest and a well-considered organising strategy and political space execute it, then it is entirely possible to transcend these divisions. Although there has been evidence of whistleblowers stepping forward to report abuses, notably in South Africa and Botswana, unlike the case of Edward Snowden, there is no real evidence in the chapters of ex-spies taking up the cudgels on behalf of the public to fight openly against surveillance abuses. This has meant that these publics lack the deep knowledge that insiders would bring to oversight and, without consistent contact with whistleblowers, they find it difficult to prove the existence of surveillance abuses, and even if they do, to act on this knowledge. Encouraging an environment where sympathetic insiders or former insiders, or spies of principles, step forward and blow the whistle on abusive practices is key, and the factionalised nature of intelligence agencies, even in more authoritarian countries, makes this possible.

Journalists are in a strong position to expose surveillance abuses, as they (except for insiders) are more likely than other sections of the publics to have access to sources in the intelligence community. However, the media is highly uneven across Southern Africa, with a strong state-owned and controlled component and relatively weak commercial and community sectors that may be risk adverse owing to their financial instability. Editors, however, enjoy social capital and can make a big difference when they act collectively against surveillance abuses, as Botswana has showed, or when the media find ways of insulating themselves somewhat from commercial pressures, by operating on a non-profit basis, opening themselves up to more public conceptions of journalism and collaborating internationally to spread the risks of reporting on surveillance abuses.

Global collaborations can also help build more democratic relationships between foreign and domestic media, particularly in former colonial countries, and prevent the kind of demobilisation evident in Angola once the immediate crisis around the 15+2 case died down. These collaborations should aim to ensure that domestic media are taken more seriously by governments, while leveraging domestic political elite's sensitivity to adverse publicity in the former colonies.

With respect to the non-media components of the public, the DRC, Mauritius and South Africa suggest that public interventions are likely to be effective if they have been constituted for a range of other purposes that bring subaltern publics into the public sphere and create space for their voices, and that allows them to relate actual or extant surveillance abuses to broader social ills. In the case of Botswana, Namibia and South Africa, where publics have been constituted in more specialist ways as networks of collaborations that share intelligence accountability and transparency as valency issues, these publics may be too narrow to exercise the social power necessary to make power-holders take them seriously. There is a clear need for civil society actors that specialise in intelligence and surveillance oversight, as the issues, and that may be constituted as NGOs with limited or no memberships. However, they are unlikely to sustain public oversight without more inclusive approach to who the affected public is and how they are constituted already for social action on diverse issues, and that generalises surveillance grievances as being part of broader problems of injustice, oppression and exploitation. As with journalism collaborations, there are clear benefits in forming more democratic international collaborations, to reshape how international organisations work in affected countries and to ensure that their interventions leave local capacity in their wake. However, as the South African case warns, an overinclusive approach towards building public oversight has its own dangers, and care needs to be taken to ensure that collaborations aim to 'get the right people in the right room with the right agenda', which is what the proposed Campaign Action Teams attempted to achieve (Right2Know Campaign 2018: 13).

OVERSIGHT

What are the tools available for public oversight? This, again, depends on the context. However, the first tool available for public oversight is space. Public oversight can utilise available media space, for example, to raise awareness about unwarranted surveillance and, in the process, mobilise communities. As Duncan states in this book, we have seen R2K in South Africa doing this. In the DRC, in South Kivu, Trésor Maheshe Musole notes that '. . . the organisation of civil society is based on the South Kivu Civil Society Charter and the internal regulations. According to Article 1er of the Charter, civil society is understood to be a grouping of structures and associations co-ordinated and organised at different levels of service to protect the vital interests of the population . . .' . Thus, public oversight mechanisms can utilise space to mobilise people and create an enduring narrative against intelligence agencies' abuse.

The Mauritius, DRC and South African case studies have shown that activists who intend to perform public oversight need to pay attention to how they frame the problem of intelligence-driven surveillance. In these cases, framings that tapped into deeper and shared social problems, and made it clear that surveillance exacerbated them, were more likely to be successful than ones that focused on individual wrongs, such as invasions of the right to privacy or violations of media freedom. Mobilisation strategies that allowed for collective responses by publics that may well have been mobilised around other constituencies and issues – for example, the churches in the case of the RAM tax in the DRC, social movements mobilised around issues as diverse as poor housing and unemployment in the case of South Africa, editors in the case of Botswana and political action, village level issues and data protection in the case of Mauritius – were more likely to win demands than those that relegated the problem to specialist groups. Nevertheless, these groups had an important role to play to explain the more technical issues around surveillance to potential publics.

What is also apparent from the successful cases is the diversity of oversight practices used. In more democratic contexts of the region, litigation is another tool for building public oversight, and strategic litigation especially can ensure that successful cases had more general benefits. Research and documentation ensured that any policy activism, including lobbying formal oversight institutions, governments or political parties, was evidence-based and supported by, at the very least, circumstantial evidence strongly suggestive of surveillance. Investigative journalism and advocacy for the information rights necessary for such journalism also added to the evidence base, with the added advantage that journalists were more likely than other members of the public to have access to sources in the intelligence establishment. In Mauritius, Chiumbu has asserted the importance of the media as a tool used to mobilise CSO actors and pressure groups against the biometrification of IDs. The media was important for awakening dormant networks and mobilising them. However, the utilisation of media space was likely to be successful if it was combined with public education and mobilisation – including picketing and pamphleteering, marches, publicity, production of media, and parliamentary and policy submissions – as these tools helped to engage broader publics beyond specialist NGO communities focusing on privacy, freedom of expression, surveillance, intelligence and/or data protection.

Where do we place parliament in this regard, as supposed elected representatives of the people and that therefore should straddle public oversight and formal oversight? The answer to this question is still not straightforward. This is because, in countries like South Africa, Mauritius and Botswana, robust debates on intelligence oversight have ensued due to an enduring culture of robust deliberative and often agonistic debates in the public sphere, and at times these debates have placed pressure on elected representatives in ways that they could not ignore as they risked losing electoral support. Mauritius, especially, is an excellent example of how surveillance can be turned into an electoral issue when the political opportunity However, parliaments that have been captured by governments or ruling parties have often ignored intelligence agency excesses. This signifies the failure of parliament as a public oversight mechanism. Yet, parliament would, one could expect, have said, 'We are the elected officials who account for the public. We should, therefore, do our job to watch over any institution with the potential to violate citizens' rights' (Former Opposition Member of Parliament in Zimbabwe, interview in Harare, 3 January 2024). In many instances, this opportunity has been missed. The failure of parliament means the failure of such an important oversight mechanism closely linked to the public.

What are the expectations of public oversight actors? In the previous sections, we have noted these expectations. For example, we have noted that oversight is meant to bring transparency and accountability to a surveillance. We have also added the need to exercise oversight of the intelligence budget, noting that, as Duncan and Munoriyarwa note in this book, failure to exercise oversight of this issue can lead to a 'Frankenstein' type of intelligence institution from which powerful individuals emerge and feed. Intelligence agencies' capabilities are defined by the technologies at their disposal. One purpose of public oversight would be to monitor the trade in surveillance technologies within specific jurisdictions. This is going to be difficult, considering the black-box nature of trade in surveillance technologies. The danger of not exercising such oversight is that some intelligence agencies may acquire technologies that may not necessarily assist with national security intelligence gathering but can be trained against legitimate political opponents at home or communities of practice like journalists. This, in turn, will protect people from arbitrary surveillance practices and the abuse of power by intelligence agencies. In some cases, though, expectations of public oversight actors have moved beyond transparency and accountability and into broader transformational objectives of ending systems of oppression and exploitation that routinely deny basic democratic rights to already socially excluded and exploited publics.

INTELLIGENCE-DRIVEN SURVEILLANCE

However, the chapters have also made it clear that in a situation where more areas of life are being digitised, the potential for digital systems to be used for surveillance purposes has grown. Therefore, what is needed is a form of public oversight that takes the diversity of surveillance practices, or practices with surveillant potential, into account. The research project on which this edited volume is based focuses on how digitisation has provided intelligence agencies with the capabilities to conduct surveillance on an unprecedented scale, and the role of public oversight in limiting the potential for abuse in circumstances where official oversight may be limited or ineffective. We have adopted this focus for the simple reason that, if misused, then these capabilities can have a massive, direct impact on the lives of citizens through, for example, repression, subversion of democratic processes and so on. At the same time, intelligence mandates have become expansive, covering a range of national security threats and interests, and which has also expanded the scope of surveillance.

As the primary focus is on intelligence-driven digital surveillance – and particularly national security intelligence where the potential for abuse is so high – it has been outside the focus of this project to examine the entire spread of public and private surveillance practices. There is one key aspect of surveillance capitalism that is relevant to this edited volume, though, namely what Shoshana Zuboff has referred to as the elective affinity between public and private missions after the September 11, 2001 terrorist attacks on the US (Zuboff, 2019, p. 116). This elective affinity arose after the attacks – and the intelligence failures that preceded them – because the intelligence community had a vested interest in collecting as much data as possible, ostensibly to prevent further failures. This convergence of interests led to unprecedented collaborations between intelligence agencies and the private sector, and to conditions for what Zuboff refers to, with reference to Giorgio Agamben's states of exception, as surveillance exceptionalism, or a situation where secret public–private intelligence collaborations are stitched together that greatly expand intelligence powers for social control purposes, while making oversight even more difficult than it was. This state of exception played out in Southern Africa too, despite being somewhat removed from the immediate aftermath of September 11, saw governments seizing on the war on terror to expand surveillance powers, although mainly in response to domestic factors.

Unprecedented public–private collaborations have greatly expanded the capabilities of intelligence agencies to collect, store and analyse data for intelligence purposes. The chapters detail the public–private interface on which so much of the surveillance architecture in Southern Africa rests. For example, SIM-card registration and data exploitation would not be possible without mobile phone cooperation with the state. Data exploitation on a massive scale in South Africa would not have been possible without compelling the involvement of the phone companies that have, on occasion, been critical of this compulsion. In this regard, China has played a key role in providing surveillance capabilities. There is a temptation for intelligence agencies to outsource or privatise more of their functions to evade scrutiny, as access to information rights tend to be weaker in relation to the private actors than the public actors. At the same time and, if pushed far enough, private companies may switch sides and defend consumer privacy if it is in their business interests to do so.

However, there is no real evidence in the chapters of private companies having played a significant public oversight role, despite the potential for them to do so, and neither is there evidence of public oversight having been brought to bear on the private sector when they strengthen unchecked state intelligence power. The fact that this is so, is unsurprising and a not entirely unjustifiable lacuna in public oversight. While these public–private surveillance collaborations have led to more distributed surveillance practices, in the cases under discussion and especially in Mozambique, Zimbabwe, Botswana and Namibia, ultimate control of these practices for intelligence purposes have also been highly centralised in presidencies and the ruling parties that control them. Therefore, oversight has focused on the legislation, policies and government practices enabling or even compelling these collaborations.

Towards a theoretical proposition on public oversight

In an attempt to develop strategies for theory-building from qualitative research, Saldana (2025) has identified six properties of theory, in that it: (1). expresses a patterned relationship between two or more concepts; (2). predicts and manages action through propositional logic; (3). accounts for parameters of, or variation in, the empirical observations; (4). explains how and/or why something happens by stating its cause(s); (5). suggests generalisability and/or transferability to related social contexts; and (6). provides insights and guidance for improving social life. The above discussion and Saldana's suggestions provides us with the building blocks for the development of a set of theoretical propositions on effective public oversight.

Developing theory is complicated by the fact that such research is difficult to generalise, especially case studies. While the research that informs this edited volume has been designed to enable generalisability through building a comparative element into it, this publication confines itself to the case-study elements. However, some general propositions around successful public oversight can still be put forward, as there are patterns that are observable from the cases. These predictions can be generalised across time and space and thereby provide guidance for actions to learn from positive experiences, while avoiding negative experiences because theory allows people to predict what works and what does not when it comes to social action (Saldana 2025, pg. 2). These propositions can be logically interconnected and culminate in a 'consequently' or 'therefore' deductive statement made by the propositions (Saldana, 2025, p. 45).

The theoretical proposition is as follows: which attempts to incorporate Saldana's six properties as well the properties that must be present for public oversight to succeed, is as follows: if NGO's with specialist knowledge of surveillance conduct public oversight of intelligence-driven surveillance in nominally democratic or weak semi-authoritarian political systems, by collaborating internationally with publicly-driven investigative journalism organisations, while building clearly defined but broad-based local capacity capable of relating surveillance to existing grievances around the oppressive and exploitative root causes of surveillance overreach, and taking advantage of any prevailing crises of democracy and resulting divisions in the political elite around surveillance overreach, then they are more likely to succeed at sustaining public oversight and achieving intelligence accountability than those that don't.

The different elements of this proposition can be explained as follows: public oversight of digital surveillance for intelligence purposes is a poorly acknowledged but important, and at times, decisive factor in the success or failure of oversight as one condition for intelligence accountability. Such oversight can be a highly effective means of calling governments to account for how they use digital surveillance and, in more authoritarian contexts, potentially the only means of doing so. Public oversight is most likely to succeed in political systems with social contracts that have been weakened or made unsustainable by high levels of inequality, coupled with oppression and exploitation, and leading to a widespread suspicion of authority and delegitimisation of state institutions, including intelligence institutions. It is also more likely to succeed in nominally democratic contexts that do not prevent the right to organise, but that lack the political will to facilitate effective formal oversight or meaningful public participation and where intelligence agencies have scope to abuse their surveillance powers, and in semi-authoritarian contexts where surveillance abuses are likely to take place, but where political alignments are unstable, state institutions are weak, and where state oversight is limited in effectiveness or even set up for failure.

Public oversight is least likely to succeed in semi-authoritarian countries which exhibit some democratic trappings, such as regular elections, but where governments exercise strong control over the levers of society, including intelligence. Public oversight is also less likely to succeed in contexts where there is strong continuity between colonial-era surveillance practices and contemporary practices, and where there has been no democratic interregnum where attempts have been made to professionalise intelligence services following a political transition from authoritarianism to one with more democratic promise. In situations where a professional, civilianised intelligence culture has taken root, then it is more likely that whistleblowers may emerge to warn about surveillance abuses, as they are more likely to be aware of the normative values of professional intelligence.

Formal oversight mechanisms, such as ministers, parliamentary committees and ombuds offices, through default or design, typically lack the resources, powers and even political will to perform oversight effectively. However, of all the formal mechanisms, the judiciary is more likely to exercise independence from the government on national security matters in situations where other official mechanisms fail and intelligence agencies are more likely to respect these decisions, particularly in nominally democratic contexts where the rule of law is more entrenched. Weak authoritarian systems may be pushed to concede demands for redress for surveillance abuses, in conditions where their survival is dependent on external relationships with international actors that are perceived to hold some kind of power over them. In strong authoritarian systems, on the other hand, they may have the opposite effect, strengthening their resolve to resist external interference. Parliaments and elected representatives may be pushed to perform oversight to limit surveillance overreach in moments when they face significant electoral competition and they fear being on the wrong side of public outrage at surveillance abuses, when political opposition commands a significant voice in political life, especially during election periods, when political competition may be heightened, or when international pressure from actors that they fear is brought to bear on them to respond to surveillance abuses, and when they fear international embarrassment.

In terms of mobilisation factors in relation to public oversight and conflict settlement once it has been exercised, collective, organised responses to surveillance overreach are more likely to be effective than individual responses. Collective responses are more likely to be effective if there are divisions in the political elite, to the point where they too fear becoming surveillance targets. These fears may increase the potential for effective public oversight as elite consensus around the need for surveillance may be weaker. The presence of NGOs specialising in issues relating to surveillance, privacy and other data rights, is an important condition for sustained public oversight, as they help to keep a constant focus on surveillance powers and capabilities. They can also play an important role in translating what may be technically complex issues into understandable messages that could be used to mobilise broad sections of society for public oversight. However, their presence alone is not sufficient for effective public oversight. The presence of mass movements supported by NGOs provides public-oversight actors with the best combination of specialist knowledge to frame digital-surveillance systems or digital systems with surveillance potential, as problems, develop informed strategies to mobilise around these problems and exercise the social power necessary to make power holders take these problems seriously and act on them. These movements do not have to be surveillance- or intelligence-focused, as they can play an important role in generalising grievances about surveillance overreach and relate them to broader societal grievances. International actors, such as international NGOs and investigative journalism organisations, can play an important and at times decisive role in forcing governments to relent on surveillance abuses but, for public oversight to be sustainable, then they need to take the building of local capacity seriously.

Other factors that may affect the success of public oversight may include a tradition of legal activism and strategic litigation in civil society, the presence of strong investigative journalism with a non-profit rather than commercial motive and an orientation towards public and collaborative, rather than competitive, journalism. At the same time, as media workers that often exercise considerable social power and that may have resources at their disposal, editors can play an important collective role in resisting surveillance abuses. The existence of surveillance victims to galvanise public support and build campaigns around, and a widespread and deeply rooted culture of activism, are additional factors and, in this regard, 'worthy victims', such as investigative journalists, are easier to organise around than victims whose occupational profiles may already be the object of suspicion, such as politicians.

Conclusion

As technologies change, actors mutate and interests shift, the question of a foolproof and totally effective oversight model of intelligence remains a far less settled question. Viitanen et al. (2012) have rightly noted how notoriously difficult it will be in the future to settle for an effective oversight model. However, by learning from the experiences discussed in these chapters and what they tell us about how the problem of surveillance overreach has arisen, what has been done about it, its causes and what happens next, it is possible to develop a guide to action that builds on what has worked, while avoiding what hasn't. And that, ultimately, is what research that attempts to engage in theory building that seeks to change the world it observes and documents, should aspire to do.

References

Butler, A. 2013. Standing up to Clapper: How to increase transparency and oversight of FISA surveillance. *New England. Law. Review.* 48, p. 55.

Gill, P. 2020. Of intelligence oversight and the challenge of surveillance corporatism. *Intelligence and National Security*. 35(7), pp. 970–89.

Halfdan, L. and Martinez i Coma, F. 2022. The effect of economic downturns on voter turnout in Africa. *Electoral Studies*. 76. [Online]. Available from: https://doi.org/10.1016/j.electstud.2022.102456. 13 May 2024. Accessed 13 May 2024

Fraser, N. 1992. Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy. In: Calhoun, C.J. ed. *Habermas and the Public Sphere*. Cambridge: MIT Press, pp. 109–42.

Johnson, L.K. 2018. *Spy watching: intelligence accountability in the United States.* Oxford: Oxford University Press.

Malgieri, G. and De Hert, P. 2017. European human rights, criminal surveillance, and intelligence surveillance: Towards 'good enough' oversight, preferably but not necessarily by Judges. In: Gray, D. and Henderson, S.E. eds. *Cambridge Handbook of Surveillance Law*. Cambridge: Cambridge University Press, pp. 509–32.

McCarthy, D.R. and Fluck, M. 2016. The concept of transparency in International Relations: Towards a critical approach. *European Journal of International Relations*. 23(2), pp. 416–40. [Online]. Available from: https://doi.org/10.1177/1354066116651688.

McIntyre, T.J. 2016. Judicial oversight of surveillance: the case of Ireland in comparative perspective. In: Scheinin, M., Krunke, H. and Aksenova, M. eds. *Judges as guardians of constitutionalism and human rights*. Cheltenham: Edward Elgar Publishing, pp. 136–62).

Murray, D., Fussey, P., McGregor, L. and Sunkin, M. 2021. Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective. *The Journal of National Security Law and Policy*. 11(3), pp. 743–70.

Newell, B.C. 2014. Technopolicing, surveillance and citizen oversight: A neorepublican theory of liberty and information control. *Government Information Quarterly*. 31(3), pp. 421–31.

Right2Know Campaign. 2018. *Second 2018 mid-term review* (report). [Online]. [Accessed 13 May 2024]. Available from: https://www.r2k.org.za/wp-content/uploads/MTR2-2018-report.pdf.

Saldana, J. 2025. *Developing theory through qualitative enquiry*. Los Angeles, California: Sage.

Van Brakel, R. 2021. How to watch the watchers? Democratic oversight of algorithmic police surveillance in Belgium. *Surveillance & Society*. 19(2), pp. 228–40.

Viitanen, P., Patama, P., Rajamäki, J.Y.R.I., Knuutila, J., Ruoslahti, H., Tuohimaa, T. and Tikanmäki, I. 2011. How to create oversight in intelligence surveillance. In: *Proceedings of the 10th WSEAS international conference on communications, electrical & computer engineering, and 9th WSEAS international conference on Applied electromagnetics, wireless and optical communications (ACELAE'11)*. World Scientific and Engineering Academy and Society, pp. 52–6.

Zuboff, S. 2019. *The Age of Surveillance Capitalism*. London: Profile Books.

INDEX

Digitisation has provided intelligence agencies with the capabilities to conduct surveillance at an unprecedented scale. Using a range of digital surveillance technologies and practices, and unprecedented public-private collaborations, intelligence agencies have extended their ability to collect, store and analyse data. Effective oversight is required to limit the potential for abuse. However, across Southern Africa – where digital surveillance is expanding – official oversight institutions typically lack the power and resources to monitor and review surveillance capabilities in order to ensure that intelligence agencies behave effectively and lawfully. Consequently, oversight in these countries typically is conducted by the public, through, for instance, challenging unjustifiable secrecy, publicising abuses and organising campaigns to rein these agencies in.

Through comparative case study research exploring lessons from key moments in the region, this volume explores public oversight of intelligence-driven digital surveillance in eight Southern African countries and examines cases where this oversight either succeeded, failed, or achieved mixed outcomes. Authored by researchers and journalists from the fields of law, communication and media studies, this book offers lessons for academics and activists, suggesting that a new model of public oversight of surveillance is possible, and, arguably, functions better than extant approaches to surveillance. It will be of global significance, as surveillance abuses are a worldwide problem, as is the problem of oversight failing to keep pace with expanding surveillance capabilities.

Jane Duncan is a Professor of Digital Society at the University of Glasgow, and she holds a British Academy Global Professorship at the same university. She is also a Visiting Professor at the University of Johannesburg. She is author of *The rise of the securocrats* (Jacana, 2014), *Protest Nation* (University of KwaZulu/ Natal Press, 2016), *Stopping the spies* (Wits University Press, 2018) and *National security surveillance in Southern Africa* (Zed Books, 2022).

Allen Munoriyarwa is an Associate Professor of Journalism at Walter Sisulu University in South Africa, in the Department of Marketing, Public Relations and Communication. His research interests are in surveillance, digital journalism, and media cultures. He has published widely in these areas. He is the co-author of *Digital Surveillance in Southern Africa: Policies, Politics and Practices* (Palgrave Macmillan, 2022).

SCOTTISH
UNIVERSITIES
PRESS

ISBN 978-1-917341-12-7
90000
9 781917 341127