KONRAD ADENAUER STIFTUNG

# THE ANATOMY OF INFORMATION DISORDERS IN AFRICA

## Geostrategic Positioning & Multipolar Competition Over Converging Technologies

By Eleonore Pauwels


JULY 2020

ISBN: 978-3-95721-706-6

# Table of Content


PREFACE iv

**EXECUTIVE SUMMARY** 1

STRATEGIC AND TAKE-AWAY MESSAGES 7

REPORT'S RATIONALE & CONTENT 8

**I - THE ANATOMY OF INFORMATION DISORDERS IN AFRICA 10**

Kenya's Emotion Wars 12

Matrix – Anatomy of Information Disorders 16

**II - AFRICA'S INTERNET OF BODIES AND MINDS 18**

Precision Political and Behavioural Engineering 19

Across Africa: Monitoring and Controlling Digital Bodies and Minds 21

**III - MANUFACTURING AND SPREADING EMOTION WARS 28**

The File is About You: Data-Mining & Profiling 31

Crafting and Advertising Violent Propaganda 32

Disinformation Architecture 33

The Power of Digital Rumours as Alternate Infospheres 35

**IV - INFORMATION DISORDERS LEADING TO SURVEILLANCE 38**

China's Biopolitics Model: Automated Ethnic Profiling 39

Every Cell Phone, A Living Brain: Controlling Information Spheres 41

The Biometrics Assemblage 44

- Within Information Disorders 45
- Within Smart and Safe Cities 47

The Global Supply Chains of Surveillance 48

**V - CYBERSOVEREIGNTY, MULTIPOLAR COMPETITION & CONVERGING RISKS FOR AFRICA 52**

State Power and Securitization Agenda 53

Multipolar Competition 55

The Sino-African Roads to Converging Tech Futures 57

Cognitive-Emotional Conflicts Waged by Russia 61

Tensions at the UN around Normative Leadership 62

**AFRICA'S GEOPOLITICAL FUTURE, EMPOWERING POPULATIONS & THE UN's ROLE 66**

Signals from the African Union, The Malabo Convention 68

Normative Leadership & Data Protection in Elections 70

**FUTURE RESEARCH AGENDA AND PRACTICAL RECOMMENDATIONS 74**

Strategic Crisis and Scenario Planning with EMBs 75

Closing the Accountability Gap and Empowering Civil Society 75

Multistakeholder Research Partnership on Hate Speech in Elections 76

References 78

Bibliography and Selected List of Expert Interviews and Consultation 90

# The Author

**Eleonore Pauwels** is an international expert in the security, societal and governance implications generated by the convergence of artificial intelligence with other dual-use technologies, including cybersecurity, genomics and genome-editing.

Pauwels provides expertise to the World Bank, the United Nations and the Global Center on Cooperative Security in New York. She also works closely with governments and private sector actors on AI-Cyber Prevention, the changing nature of conflict, foresight and global security. In 2018 and 2019, Pauwels served as Research Fellow on Emerging Cybertechnologies for the United Nations University's Centre for Policy Research. At the Woodrow Wilson International Center for Scholars, she spent ten years within the Science and Technology Innovation Program, leading the Anticipatory Intelligence Lab. She is also part of the Scientific Committee of the International Association for Responsible Research and Innovation in Genome-Editing (ARRIGE). Pauwels is a former official of the European Commission's Directorate on Science, Economy and Society.

Pauwels regularly testifies before U.S. and European authorities including the U.S. Department of State, NAS, NIH, NCI, FDA, the National Intelligence Council, the European Commission and the UN. She writes for Nature, The New York Times, The Guardian, Scientific American, Le Monde, Slate, UN News, The UN Chronicle and The World Economic Forum.

# Preface

Elections are a key element of any democracy. However, we have seen in the past the fallacy of electoralism[1] and the temptation by many external actors to declare a political system as democratic just because of regular electoral exercises. Often the quality of elections as such has been disregarded, or deficiencies in the electoral process were identified but persist without any consequences. According to widely recognized international standards democratic elections have to be free, meaning the rights of citizens to participate and to compete are respected and protected by the rule of law. Democratic elections are equally meant to be fair, meaning that a level playing field should exist. But what do these minimal standards mean in the age of artificial intelligence, new technologies and what Eleonore Pauwels, the author of the present study describes as information disorders?

For a political foundation such as Konrad-Adenauer-Stiftung who has in its mandate the support of democratization processes worldwide, the impact of new technologies on electoral processes and the state of our democracies is of utmost interest.

It affects consolidated as well as emerging democracies. The threats that we are facing are manifold and they go way beyond the erosion of institutions. They particularly impact and dramatically change the social fabric and the political culture in our societies. A transformation that certainly also has its positive sides as long as the negative side-effects and collaterals are reigned in. But particularly the latter has never been as complex before.

In defense of democracy we can identify two frontlines:

We have the political space, the ambit where candidates and parties are campaigning, seeking popular support and where online defamation, hate-speech, data leaks, disinformation and deep-fakes can alternate the level playing field. It is this level, the capturing of the hearts and minds of citizens, which the present study "The Anatomy of Information Disorders in Africa" dissects in detail and illustrates with examples from the African continent.

But we also have the technical space where particularly Electoral Management Bodies are the most vulnerable institutions. It is a sphere where data manipulation by local or foreign actors can disrupt an electoral process, and where competing political parties need to have sufficient expertise on technologies used in order to understand and to prevent any electoral fraud.

In order to gain further insights into the vulnerability of the electoral cycle to modern technology, KAS New York embarked together with the author of this study on a broader research project that besides of the use of AI to generate hyper-targeted disinformation campaigns, data-manipulation and cyber/AI-enabled cognitive-emotional conflicts and disinformation also addresses pertinent questions such as how fit for purpose are electoral laws in the context of today's technological abilities? And how can security and resilience of election infrastructure be guaranteed best?

The results of these analyses are meant to assist and to sensitize Electoral Management Bodies, law makers, political party representatives, media and civil society to the emerging threats which jeopardize the democratic character of elections and bring about wide-spread repercussions for the political culture of societies.

It also reaches out to international organizations who often assist in election management or election observation and who need to take into account the possible distortions which easily might get unnoticed.

KAS New York wishes all stakeholders and the interested public an interesting read!

**Andrea E. Ostheimer**
Executive Director
Konrad-Adenauer-Stiftung, New York

[1] A term coined by political scientist Terry Lynn Karl.

# Executive Summary

We face an era of "emotion wars," where algorithmic networks in our social media spheres electrify millions of brains to amplify emotions, hate and distrust.

Emotion wars are lucrative, produced for several millions of U.S. dollars by corporations in the political consultancy business. They spread fast, targeting the minds of populations across the globe. In the Unites States, the resentment of African American communities against police violence is fuelled by Russian troll factories delocalized to Ghana.[1] In India's West Bengal region, Rohingya refugees, who fled exactions in Myanmar, are now demonized in violent speech that rapidly metastasize on WhatsApp.[2] In South Africa and Kenya, disinformation and hate speech manufactured, in part, by political elites, inflamed the racial and socio-economic divisions that have plagued both countries for decades.[3]

Emotion wars are an existential threat to democracy, increasingly manipulating the course of elections, undermining citizens' political agency. In Kenya's 2013 and 2017 elections, divisive and inflammatory online propaganda, including graphic violence, targeted ethnic and socio-economic population subgroups, invading mobile phone and social media networks as well as traditional media.[4]

Each election witnessed more refined and precise strategies for controlling spheres of information and exploiting political and emotional engineering targeted at segmented communities. Such strategies were crafted with the support of foreign data-analytics companies, Cambridge Analytica and the SCL Group,[5] for profiling and influencing voters' behaviours. Their prime targets were young Kenyans who had grown up with the viral and addictive forces of virtual networks. Yet, major political parties, the ruling Jubilee party and the opposing National Super Alliance (NASA), had also built and deployed widespread communication architecture to target specific segments of the Kenyan population.

This is where we stand. Just as the Internet has reshaped commerce, politics, social fabrics and the stories we tell, it now interferes more directly than ever with how we process and interpret knowledge and information. The era we face – where artificial intelligence (AI) and data-capture technologies converge to analyse our digital bodies and minds – is an epistemic revolution as much as a technological one.

This report is an attempt to make sense of this transformative shift – to analyse its nature, identify its rules, and understand its effects. The report focuses on what scholarship calls information disorders and their impact on elections in several African countries, including Kenya, Nigeria and South Africa. Delineating the anatomy of *information disorders*[6] in countries across Africa is a less chartered, but timely story, as analysts have often focused on information operations in the West.

## The Anatomy of Information Disorders in African Elections

African societies are about to face an unprecedented transformation powered by the integration of AI and data-optimization technologies into politics, daily life and elections. Since the spring of 2019, nearly 40 million Kenyans had their fingerprints and faces scanned by a new biometric ID system that will play a crucial role in the next 2022 election.[7]

In 2020 and 2021, several African nations will go to the polls, for both legislative and presidential elections [Map 1]. These include Ghana, Ethiopia, the Central African Republic as well as countries in the Sahel that face increasing unrest, terrorist threats, migrations and potential Russian interference in elections. Authoritarian regimes in Egypt, Burundi, Tanzania will have elections in 2020 and Uganda and Zambia in 2021. Elections might be disrupted by the ongoing pandemics that erupted beginning of 2020. Such context of global instability and distrust will only amplify threats to the integrity of nations' political processes.

This report aims to explain why and how information disorders contaminate elections in Africa, eroding citizens' trust in governing institutions, and to prepare us for what is emerging next.

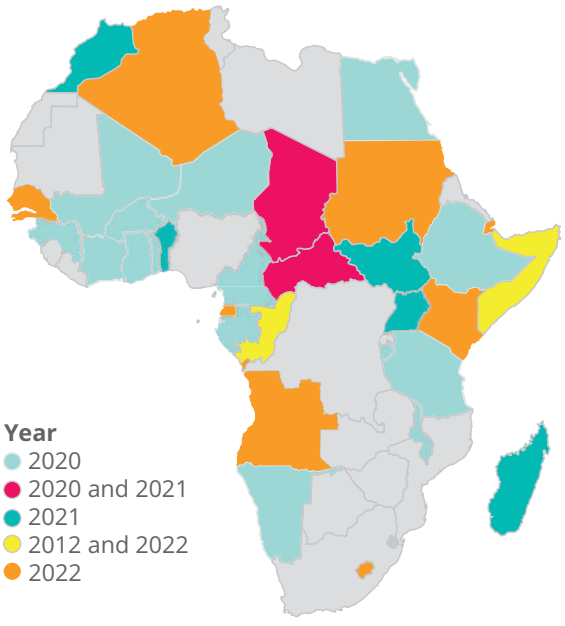
The global development agenda seeks to realize the promises of the digital economy, bringing prosperity, inclusion and empowerment. Biometric and digital ID systems are making exponential advances across the African continent, with many nations in the process of registering their populations' biometrics into centralized national databases [Map 2]. Other converging technologies – from facial and affect recognition to surveillance tools for monitoring social media content – are increasingly used by authorities to track populations' behaviours, literally "taking the pulse" of the electorate. For instance, in February 2019, the French company, Gemalto, announced a smart-policing collaboration with the Uganda Police Force to deploy portable biometric devices that use AI to confirm a match on the spot.[8]

When studying the impact of information disorders on elections, we tend to seriously underestimate how converging technologies are increasingly designed to anticipate and nudge human attitudes and behaviours, with the drastic potential to manipulate and restrict political agency. The convergence of AI with pervasive facial, biometrics and affect recognition essentially allows new forms of political, social and behavioural engineering.

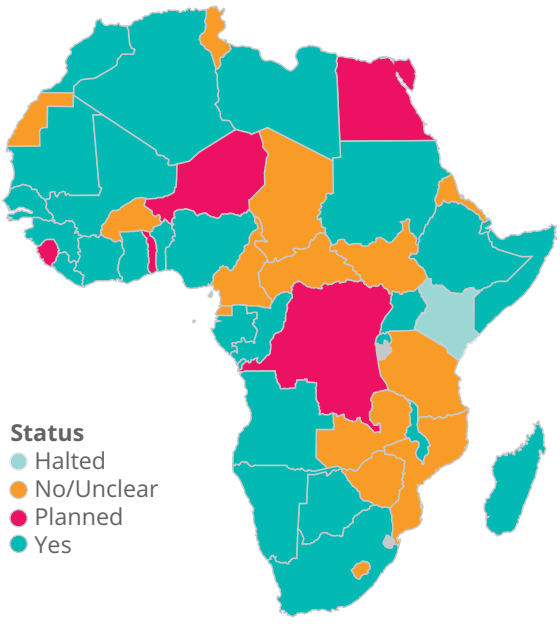
Converging technologies monitor and analyse individuals' biometrics and behavioural data, gradually imposing social and political control over those individuals' lives. Such "power over life" resonates with what French philosopher, Michel Foucault, termed *biopower*: "[A] power that exerts a positive influence on life, that endeavours to administer, optimize, and multiply it, subjecting it to precise controls and comprehensive regulations."[11] In an era of technological convergence, algorithms essentially amplify biopower, augmenting technologies' potential to regulate societies' collective body.

In several countries in Africa, these new forms of political and social controls are born out of the complex alliance between a host of actors, from foreign tech-leading nations, domestic ruling elites, to Western corporations that prosper in the data-analytics and political consultancy business. These actors' collusive practices thrive in societies where data and technological governance suffers from a lack of robust regulatory and oversight mechanisms. A dearth of normative capacity-building and meaningful accountability has left populations and civil society

**Map 1** | Scheduled Presidential or National Assembly Elections[9]




**Map 2** | Implementation of Biometric National Identification System[10]



organisations in several African countries, vulnerable to dynamics of power-, data- and resource-capture.

**Four powerful technological, political and geostrategic trends** contribute to the proliferation and amplification of information disorders in African elections. Such trends form the anatomy of what this report calls "cognitive-emotional conflicts" or "emotion wars," new forms of political and social engineering, exploiting data and digital technologies, to control and manipulate populations.

- The first trend is the increasing capacity and willingness of ruling governments in Africa to instrumentalise digital networks for inflaming existing racial, social and economic divisions between subpopulations. In Kenya, Nigeria and South Africa, campaigns to "monitor and influence the pulse" of the electorate have focused on aggravating these cleavages.

- The second trend is closely interconnected with the exploitation of racial, ethnic and economic tensions. In countries where privacy and data protection laws are not translated into robust operational mechanisms, state and private sector actors can extract sensitive personal data from an array of online population databases for targeting ethnic and socio-economic groups. Relying on the aggressive, incendiary campaigns generated by PR companies like Cambridge Analytica, domestic political parties can exploit citizens' personal profiles and information networks for spreading rumours, targeted propaganda, hate speech, mis- and disinformation[12]. The rationale behind such sophisticated disinformation architecture is to immerse citizens in an alternative, virtual reality where they themselves become producers of digital manipulation. In Africa, the capacity to manipulate populations and information is increasingly imposed through the "Internet of Bodies and Minds."[13]

- Third, monitoring and controlling human populations is the result of a securitization agenda where converging technologies help state actors impose surveillance and repression. The tactics and tools of digital surveillance can be harnessed for both, fuelling information disorders in elections and repressing professional groups that offer resistance, such as traditional press and civil society.

  For several states in Africa, facing rising domestic pressure, the ability to control spheres of cyber-influence and information infrastructures is part of a "survival strategy" to preserve regime stability. These governments have direct interest in overseeing and censoring content and information that could undermine, even imperil, domestic stability and regime legitimacy. In recent years, a series of cybersecurity legislation have been proposed and passed by Kenya, Nigeria, and other states in the name of defending and protecting national interest in the fight against terrorism, even if, at times, such legislation violates individual rights.[14] Beyond violations of human rights and freedom of expression, national security measures have gradually led to a shrinking of civic space. Today, the risk for populations is the closing of "virtual civic space."

- Fourth, when foreign countries or corporations engage in spreading information disorders in faraway fragile nations, they are often incentivized by a long-term agenda of power and resource capture.[15] This is obvious in African countries where foreign companies collude with political and economic elites for the shaping of electoral outcomes. These foreign companies are promised access to growing markets and industries, involving data, oil, genetic and biodiversity resources, rare earth minerals and metals. Increasingly, interference by foreign interests is not confined to influencing elections. For years and in dozen African countries, corporations of lobbyists and data-brokers like the SCL Group have been analysing data about African populations, from health, nutrition, sanitation, weapons to militarized youth.[16] These political consultancy firms are part of what this report calls the "global supply chains of surveillance." And the sensitive datasets they collect give them and other companies to whom the data is auctioned off, more influence in the current race for strategic positioning in Africa.

The above four trends form the anatomy of information disorders. And these trends are actually happening in most countries – Kenya, Nigeria, South Africa, India, Malaysia and Brazil – that have been targeted by companies in the political consultancy business.

Yet, this report is also an urgent call for considering the far-reaching geopolitical implications we face at the intersection of several transformative shifts: a multipolar competition for mastering converging technologies; the rise of cyber-sovereignty as an emerging governance model for nations, increasingly distancing themselves from the West; the crucial importance of the African continent as a geostrategic market for positioning and controlling of tech futures; finally, the challenge of normative leadership and, ultimately, the relevance of the multilateral system and its capacity for norm setting.

## Africa's Geostrategic Importance in a Multipolar Competition

The report therefore depicts the wider geopolitical story behind the instrumentalization of information disorders in elections across Africa. This is a story in three acts, with ramifications for state-power, cyber-sovereignty, and geo-strategy.

- Like metastases on the global map, information disorders seem to rapidly contaminate the Global South, affecting elections in both, fragile democracies and authoritarian states. Yet, the tools of epistemic and emotional manipulation do not randomly spread through the wired bloodstream of global connected platforms. In African nations, the convergence of AI and data-capture technologies is harnessed by state-power, not only for manipulating populations' behaviours in elections, but for strengthening regimes through pervasive algorithmic surveillance, repression and control. Algorithmic and biometrics platforms – the biometrics assemblage – serve powerful securitization agendas.

  Increasingly, populations and civil society in Kenya, Nigeria and South Africa are questioning the tensions around the digital economy's social contract: What is the balance between individual rights and state-command of collective security and prosperity in the digital economy? Policymakers across the world face this question, but in several African countries where population-wide biometrics ID projects have started without robust data-protection oversight, it is being posed with urgency.

  In Kenya, Nigeria and South Africa, 2019 has witnessed nascent normative efforts around privacy and data-protection.[17] What is at stake is a competition between the values of liberal democracies with new forms of digital authoritarianism. The commodification of massive streams of populations' data means that, in the future, governments may be able to not only monitor and control the behaviours of individuals, groups, professions and media communities, but also produce economic value to be redistributed. The risk is that digital authoritarian regimes could become models to ensure ruling elite preservation – with its dynamics of resource capture – and provide both, growth and security under a repressive social order.

  Interestingly, the question of data protection radiates back into the international arena because, in the global digital economy, population data flow across borders. A rising concern for policymakers, diplomats and CEOs with global reach, is the risk to face increasing competing visions of governance and a balkanization of cyberspace with diverging standards on privacy, security, free speech, and cross-border data-transfers. As data protection laws emerge in countries in Africa, governments might impose tighter national control of the internet, for instance by adopting China's data-localization principles, requesting data to be stored in the country of origin. This is why we currently witness a race between U.S. and Chinese technological platforms to build data centres and information infrastructures on strategic territories – coastal cities and resource-hotspots – in African countries. In February 2019, Huawei launched its first data centre in Egypt, which conveniently borders the corridor that connects East Africa to Europe. The Chinese telecom also signed a contract with the Algerian government to build a data centre for its custom and border authority. With BRI agreements signed with Morocco, Algeria, Tunisia and Egypt, China has a footprint in the Mediterranean.[18]

Regulatory moves towards data-localization and cyber-sovereignty would make it increasingly difficult for the United Nations and its agencies (like the World Health Organisation) to rely on global data-sharing to address shared problems such as mitigating the consequences of pandemics. This is another complex governance problem, which the United Nations will have to address if the institution wants to stay relevant when it comes to crisis prevention and global development.

- Increasingly, national elections can be influenced to define what model of cyber-sovereignty will prevail on the world' stage. Once, primarily, a strategic moment in a country's national political process, each election now provides foreign tech-leading nations with an opportunity to shape technological and data-governance models, and to play a role in the global historic definition of cyberspace.

  In African countries particularly, information disorders during elections start demonstrating the endorsement of the Sino-Russian model of cyber-nationalism up to a normative scale. Such normative influence is based increasingly on close ties with China that helps to build and, more importantly, to control technological, information and resource infrastructures. While lacking China's economic power and cyber-diplomacy, Russia relies on ad hoc political engineering of campaigns to degrade social cohesion among African populations, create instability and carve specific sectors for resource-capture. Russia's most obvious and successful interference in Africa targeted the far-away island of Madagascar.[19] The operation was orchestrated for the Kremlin by Russian agents linked to Yevgeny Prigozhin, the oligarch accused of interfering in the U.S. 2016 elections.

  While countries like Kenya, South Africa and Nigeria are already deploying, with success, transformative financial services in the digital economy, they still face sustained economic and capacity building challenges, and as importantly, weaknesses in governance. They are therefore likely to partner with tech-leading nations to build the required information infrastructures and import the converging technologies' expertise needed to secure further integration into the global digital economy. The countries they choose to partner with will inevitably bring and potentially impose, specific technical standards, proprietary agreements and normative governance.

  At the same time, on the global scene, Kenya, Nigeria and South Africa represent an Eldorado of growing digital markets, with access and control over large populations' data, as well as energy and mineral resources needed to power the digital economy. Even more, these countries constitute different geostrategic territorial corridors where to build future 5G digital architectures as well as cloud-computing and satellite data centres. Within a context of rising multipolar competition, governments in Kenya, Nigeria and South Africa will determine which governance model is going to help them secure relative economic growth and autonomy without endangering regime stability. China's cyber-sovereignty model emerges as a potential option, which applies cyber-surveillance to preserve regime legitimacy and prevent external threats.

## Empowering African Societies and the Future of Multilateralism

In a world in which states and corporations increasingly partner to monitor populations' behaviours and their information networks, how can the United Nations (UN) provide normative leadership to help promote populations' data protection and therefore protect human rights? In particular, can UN agencies gather member states' support to prevent the rising forms of political data-collection and manipulation that impact populations through information disorders and electoral disruptions?

In the absence of adequate laws, policies, and corporate practices that are grounded in internationally recognized principles for human rights, the most intimate data we share can be used to undermine democratic processes and hurt citizens, in particular, the most vulnerable among us.

A timely and crucial diagnosis is that, in the race to achieve the promises of the digital economy, we face a pervasive, harmful gap between our normative frameworks and the implementation of meaningful accountability. This is essentially a failure, an incapacity to translate high-level ethical declarations into viable normative mechanisms that can ensure meaningful accountability, for an array of populations, with their particular vulnerabilities, but also their normative socio-cultural contexts.

In 2020, 24 African countries out of 53 are in the process of adopting or updating laws and regulations to protect citizens' personal data.[20] This is where the African Union (AU) and the UN could play a unique role in normative leadership. Both institutions provide a forum where public and private sector actors, in collaboration with civil society, could perform what the author calls "normative foresight." Such foresight effort would focus on multistakeholder collaborations to translate high-level principles of personal data protection laws into operational, accountable mechanisms and practices. They will also need to stress-test these normative practices in the context of different scenarios where privacy could be breached and personal data abused, resulting in human right violations. Civil society actors, policymakers and data-protection experts from Kenya and Nigeria might be crucial partners to include in this effort of normative guidance.

In a 2019 landmark report for the UN University, the author proposed to equip the UN with a global foresight observatory, which would develop a responsible governance approach to harness AI and converging technologies for the UN conflict prevention agenda and for social empowerment.[21] This global observatory could foster tailored collaboration to support civil society organisations, digital rights labs and young innovators in Africa in their effort to build governance accountability models that meet the ethical needs of African democracies.

In this brokering function, an array of entities within the United Nations system could play a role that is sorely needed at the international level: 1) support to negotiate adequate normative frameworks for populations' data-protection, privacy and digital rights; 2) normative foresight to better implement data-protection mechanisms, which are tailored to African countries' challenges; and 3) the development of strategic monitoring and crisis planning capacity for electoral management bodies to help mitigate the impact of information disorders in elections and the risks of their own data manipulation.

Still the risk exists that, in the near-future, tech-leading nations and their corporate partners will increasingly instrumentalise the UN mandate in normative and technical capacity-building to crystallize their competitive advantage (through standards and proprietary technologies) and augment their control over transnational cyberspace infrastructures.

Beyond the internet of bodies and minds, states' competition is also about amplifying spheres of normative influence through discursive power and the cyber-stories they tell. The race for showing governance leadership, through narratives and actions, is clear during the pandemic that erupted in the beginning of 2020. China, for instance, tried to eclipse foreign fears and resentment about the dramatic global impact of Covid-19 with soft power, by sending medical equipment to European countries that were too burdened to share supplies within their internal market's borders.[22] Domestically, videos of hospitals built in haste were supposed to provide virtual consolation to China's affected populations.[23]

The UN will not be immune to rising attempts at using soft discursive power and information disorders to weaken the traditional values and norms of multilateralism. This era of information disorders and "emotion wars" strongly affect trust in the multilateral order and in the UN leadership to protect global populations, not only from technological and biological threats, but also from surveillance, digital and epistemic manipulation. For the UN, the only way ahead to preserve relevance is to provide forward-looking and robust normative leadership, partnering with the next-generation of civil society and private sector actors to empower populations across the world. Visionary normative leadership is needed.

We live in an age where AI technologies augment the potential of what Foucault termed "biopolitics,"[24] a series of interventions and regulatory controls aimed at constantly monitoring information about large populations. The supremacy to use algorithmic information networks to manipulate populations' beliefs, attitudes and behaviours within and beyond your borders is today the most strategic way to gain material and global power.

# STRATEGIC & TAKE-AWAY MESSAGES

Societies across Africa face an unprecedented revolution powered by the integration of AI and data-optimization technologies within politics and society.

State and private sector actors involved in African elections exploit the combination of AI and populations' sensitive data to exert new forms of political and social engineering.

In an increasing number of African countries, monitoring and controlling populations serve a securitisation agenda where converging technologies help state actors to impose surveillance and repression.

The geopolitical risk is for those African nations to adopt China's governance model based on cyber-sovereignty. In China's geostrategic positioning, Africa features at the centre of a rising multipolar competition to ascertain control over the transnational information infrastructure of the global digital economy.

If multilateral institutions aim to stay relevant in addressing shared problems, from preventing pandemics to mitigating climate change, they need to exert normative leadership to help empower and protect African populations in the digital economy.

# Report's Rationale & Content

This report aims to analyse the anatomy of information disorders and their impact on elections in several African countries, including Kenya, Nigeria and South Africa. It also demonstrates why and how influencing elections in Africa is critical for geostrategic positioning in an era of rising multipolar competition. This wider geopolitical story has significant ramifications for state-power, cyber-sovereignty, and the future of multilateralism.

**Section I** of the report provides a condensed analysis of some of the overarching technological, political and geostrategic trends that contribute to the proliferation and amplification of information disorders in African elections. These trends form the **anatomy of information disorders** – also called "cognitive-emotional conflicts" or "emotion wars" – new forms of political and social engineering, exploiting data and digital technologies, to monitor and control populations. Section I also offers a succinct overview of how the above-mentioned four trends have impacted Kenyan elections. Next sections present more in-depth case-study analyses, involving Kenya, Nigeria and South Africa.

**Section II** explores a major paradigm – **Africa's Internet of Bodies and Minds** – in which African societies face an unprecedented upheaval powered by the integration of AI and data-optimization technologies into politics, daily life and elections. Across countries in Africa, biometric, algorithmic and digital ID systems centralize populations' sensitive data with the opportunity to provide access to essential public services. But, in context where robust oversight of human rights and data protection is lacking, such systems create pervasive risks, from crystallizing discrimination to the exploitation of personal information for electoral gain. Most troubling perhaps are failures to ensure accountability and responsibility for risks, in particular when those technologies are used in elections. Implications for populations' privacy and agency could be corrosive. Equipped with the technological tools to analyse and control how humans act upon information and knowledge, government and corporations involved in Africa's elections can increasingly monitor and influence populations' attitudes with the drastic potential to manipulate and restrict political agency.

**Section III** focuses on case-studies in Kenya, Nigeria and South Africa to examine the digital manipulation machine behind **"Manufacturing and Spreading Emotion Wars:"** 1) building voters' profiles using leaked, sold or un-encrypted data from large government and private services databases; 2) crafting vivid, even graphically violent propaganda that exploits ethnic and socio-economic tensions to target segments of the electorate defined by ethnicity, political leanings and age; 3) relying on networks of surrogates to inundate information spheres such as private messaging applications as well as TV, radio, and social media; 4) running powerful digital ad campaigns and tweaking algorithmic search engine and algorithmic content-regulation on social media platforms; 5) silencing resistance by capturing or waging a war on traditional media structures.

**Section IV** illustrates how information disorders play a role in a larger securitization agenda. This section provides a detailed account of how African states harness converging technologies, including AI and biometrics, facial and affect recognition, for political and social control. It also unveils the influence of China's social credit system on African societies and describes the **Global Supply Chains of Surveillance**. By constantly monitoring "traceable bodies and minds," such biopolitics forces exert and amplify dynamics of exclusion and discrimination imposed on populations that are already vulnerable.

© Unsplash/Veit Hammer

> National elections can be influenced to define what model of cyber-sovereignty will prevail on the world' stage.

**Section V** demonstrates how information disorders are symptomatic of a wider multipolar competition for normative influence in cyberspace. Governments in Kenya, Nigeria and South Africa have to decide what cyber-governance model will help project sovereignty, while leading towards economic and security autonomy. And the governance options they will take increasingly depend on the tech-leading nation they partner with. This section provides an in-depth analysis of the **Sino-African Roads to Converging Tech Futures**, following China's Belt and Road Initiative.

The conclusion offers a future research agenda for the UN and electoral management bodies. It finally reflects on the role that the multilateral system could play to help empower African societies to prevent digital and electoral manipulation: 1) support to negotiate adequate normative frameworks for populations' data-protection, privacy and digital rights; 2) normative foresight to better implement data-protection mechanisms, which are tailored to African countries' challenges; and 3) the development of strategic monitoring and crisis planning for electoral management bodies to help mitigate the impact of information disorders in elections.

© UN Photo/Marco Dormino

# THE ANATOMY OF INFORMATION DISORDERS IN AFRICA

The global development agenda aims to realize the promises of the digital economy, bringing prosperity, inclusion and empowerment. Biometric and digital ID systems are making exponential advances across the African continent, with many nations in the process of registering their populations' biometrics into centralized national databases [Map 2]. Other converging technologies – from facial and affect recognition to surveillance tools for monitoring social media content – are increasingly used by authorities to track populations' behaviours, literally "taking the pulse" of the electorate. For instance, in February 2019, the French company, Gemalto, announced a smart-policing collaboration with the Uganda Police Force to deploy portable biometric devices that use AI to confirm a match on the spot.[25] In 2018, the government of Zimbabwe invested in emerging technologies to deploy networks of CCTV cameras connected with facial-recognition software across cities' infrastructure.[26] In the streets of Johannesburg, the AI software iSentry, paired with facial recognition and webs of CCTV cameras, is programmed to detect and interpret "abnormal behaviour," pointing to the risk of automated forms of predictive policing.[27]

In several countries in Africa, these new forms of political and social controls are born out of the complex alliance between a host of actors, from foreign tech-leading nations, domestic ruling elites, to Western corporations that prosper in the data-analytics and political consultancy business. These actors' collusive practices thrive in societies where data and technological governance suffers from institutional and regulatory frailty. A lack of normative capacity-building and meaningful accountability has left populations and civil society organisations in several African countries, vulnerable to dynamics of power-, data- and resource-capture.

The harmful tactics of PR strategists and data-brokers with global reach – from Cambridge Analytica, SCL Group to Bell Pottinger – have led to condemnation, outrage and distrust.[28] But the toxic work of these corporate data barons is only one piece of a larger story unfolding in Africa and the rest of the Global South.

Four powerful technological, political and geostrategic trends contribute to the proliferation and amplification of information disorders in African elections. These trends form the anatomy of what this report calls "cognitive-emotional conflicts" or "emotion wars," new forms of political and social engineering, exploiting data and digital technologies, to control populations.

**Political and Emotional Engineering Exploiting Societies' Tensions:** The first trend is the increasing capacity and willingness of ruling state actors in Africa to instrumentalise digital networks for inflaming existing racial, social and economic tensions between subpopulations. These emotion wars can be orchestrated by political parties themselves or crafted by the foreign data-analytics companies they hire within lucrative contracts. Information disorders have had powerful ramifications in an array of nations, including in the UK and U.S., sowing distrust and polarization.[29] But, populations in Africa that have suffered long-lasting violent crises and ethnic cleavages and have low levels of education, are particularly vulnerable to political and social engineering through the weaponization of social media.[30]

> "Populations in Africa that have suffered long-lasting violent crises and ethnic cleavages are particularly vulnerable to political and social engineering through the weaponization of social media.

**Exfiltrating Sensitive Populations' Data for Targeting:** The second trend is closely interconnected with the exploitation of racial, ethnic and economic tensions. In countries where privacy and data protection laws are not translated into robust operational mechanisms, state and private sector actors can extract sensitive personal data from an array of online population databases for targeting ethnic and socio-economic groups. Relying on the aggressive, incendiary campaigns generated by PR companies like Cambridge Analytica, domestic political parties can exploit citizens' personal profiles and information networks for spreading targeted propaganda, hate speech, mis- and disinformation. In Africa, this capacity to control populations and information – a new form of "biopolitics"[31] – is increasingly imposed through the Internet of Bodies and Minds.

**Networks of Precision Surveillance and Repression:** Third, monitoring and controlling human populations is made possible by a securitization agenda where converging technologies help state actors impose surveillance and repression. The tactics and tools of digital surveillance can be harnessed for both, fuelling information disorders in elections and repressing communities that offer resistance, such as traditional press and civil society.

> "The tactics and tools of digital surveillance can be harnessed for both, fuelling information disorders in elections and repressing communities that offer resistance.

**Strategic Positioning for Resource and Power Capture:** Fourth, when foreign countries or corporations engage in spreading information disorders in far-away fragile nations, they are often incentivized by a long-term agenda of power and resource capture.[32] This is obvious in African countries where foreign companies that collude with political and economic elites for electoral shaping are promised access to growing markets and industries, involving data, oil, biodiversity resources, rare earth minerals and metals. Increasingly, interference by foreign interests is not confined to influencing elections. For years and in dozen African countries, corporations of lobbyists and data-brokers like the SCL Group have been analysing data about African populations, from health, nutrition, sanitation, weapons to militarized youth.[33] They grow what this report calls the "global supply chains of surveillance." And the sensitive datasets they collect give them and other companies to whom the data is auctioned off, more influence in the current race for strategic positioning in Africa.

The above four trends form the anatomy of information disorders. And they are actually happening in most countries – Kenya, Nigeria, South Africa, India, Malaysia and Brazil – that have been targeted by companies in the political influence business. Beyond lucrative pay-offs, such trends might even constitute the kind of criteria that companies like Cambridge Analytica and the SCL Group would consider when weighing their engagement in and with countries in the Global South.[34]

Recent elections in Kenya provide vivid, powerful examples to understand the anatomy of information disorders in Africa. Below is a succinct overview of how the above-mentioned four trends took place in Kenyan elections while next sections will present a more in-depth analysis.

## KENYA'S EMOTION WARS

**Weaponizing Racial, Social and Economic Tensions** – Kenya's 2007/2008 elections ended up in violent outbursts that killed over 1,000 people and displaced over 600,000.[35] The 2013 elections were marred by the rise of online hate speech that inflamed ethnic tensions.[36] The 2017 election result was annulled and rerun in context of heightened insecurity, with a death toll of about 100 people and the death of a senior election official.[37]

Kenya has suffered decades of ethnic conflicts, terrorist threats and economic inequality. One of the main findings of the Commission of Inquiry into the 2007 Post-Election Violence, also called the Kriegler Commission,[38] is that the 2007 post-election violence burst spontaneously in some geographic areas and was carefully planned in other areas, often with the involvement of political and economic elites. Some regions witnessed a combination of the two forms of violence, where violent reaction to the per-

> Each election witnessed more refined and precise strategies for controlling spheres of information and exploiting political and emotional engineering targeted at segmented communities.

ceived rigging of elections spread widely, in particular through hate speech on vernacular radio stations. It later evolved into coordinated attacks on members of ethnic groups associated with the incumbent president or the main opposition party.

The Kriegler Commission's report concludes that the post-election violence consisted in systematic attacks targeting Kenyans based on their ethnicity and their political leanings. The dissemination of rumours, hate speech and incitement to violence had sinister, dramatic ramifications. Attackers organized along ethnic lines, with substantial logistical means, and assaulted population subgroups because these were of particular ethnicity and political persuasion or association.


"Secretary-General Ban Ki-moon (centre, head table), flanked by Kofi Annan (left, head table), former United Nations Secretary-General, and Anna Tibaijuka, Executive Director of the United Nations Human Settlements Programme, in a meeting to end the deadly violence sparked by recent disputed results of the presidential elections, with the major parties to the conflict." (01 February 2008)

In 2013 and 2017, divisive and inflammatory online propaganda, including graphic violence, targeted ethnic and socio-economic population subgroups through mobile phone and social media networks as well as traditional media.[39]

Each election witnessed more refined and precise strategies for controlling spheres of information and exploiting political and emotional engineering targeted at segmented communities. Such strategies were crafted with the support of foreign data-analytics companies, Cambridge Analytica and the SCL Group, for profiling and influencing voters' behaviours.[40] Yet, major political parties, the ruling Jubilee party and the opposing political group called the National Super Alliance (NASA), had also built and deployed a widespread communication architecture to target specific segments of the Kenyan population.[41]

> In the run up to the 2017 elections, WhatsApp groups, including non-political ones, were inundated with incendiary ethno-nationalist rhetoric, mis- and disinformation.

In the run up to the 2017 elections, WhatsApp groups, including non-political ones, were inundated with incendiary ethno-nationalist rhetoric, mis- and disinformation.[42] A significant number of social media groups already existed or were formed along perceived ethnic voting blocs. Microtargeted propaganda therefore relied on assuming users' political leanings based on their names and ethnicity. For instance, members of a certain ethnic group would receive propaganda threatening to annihilate their tribes, producing fear of mobilization and voters' suppression.[43] Disinformation campaigns also exploited existing fears surrounding election-related violence, terrorist group Al-Shabab attacks and disease outbreaks. In a country with an history of interethnic conflicts, religious tensions and terrorism, campaigning based on aggressive ethnic profiling has hurtful, fatal implications.[44]

**Exploiting Populations' Databases** – Recent research by Kenyan scholars points to several plausible sources of population and personal data that

have allegedly been mined in the course of the 2017 elections.[45] In 2018, media reporting found that staff members at Kenya's Independent Electoral and Boundaries Commission who were mandated to protect voter data made millions of Kenyan shillings by illegally selling private voters' data to politicians during the 2017 general election. In a 2018 report from Strathmore University's Centre for Intellectual Property and Information Technology (CIPIT), Kenyan expert, Robert Muthuri, explains how both major campaigning parties gained access to personal voters' data to target them with large amounts of unsolicited political text-messages (p 5): "We posit that the data-involved in such mining included voter registration data, particularly, the names and addresses of potential targets. In Kenya, such targeting is easier because peoples' names disclose their ethnic background."[46] Voters' registration information was subsequently connected to social media profiles and mobile phone numbers to achieve more precise targeting within personal networks.

The consequences of exfiltrating data from national population databases used for voter registration, as well as public and private services, could be corrosive. The entire digital identification history of individuals and populations – in intimate granularity, from ethnic background, wealth status, residence, online behaviours, political and sexual orientations – could be leveraged for targeted propaganda, intimidation and discrimination.

> The growing surveillance apparatus plays a substantial role in information disorders, from discrediting traditional media, to silencing civil society actors.

**Expanding Surveillance Apparatus** – Surveillance of individuals – often journalists, activists, opposition figures, critics and others exercising their right to freedom of expression – has thrived in Kenya, including at election times.[47] The growing surveillance apparatus plays a substantial role in information disorders, from discrediting traditional media, to silencing civil society actors that report human rights breaches. As the Kenyan government is the largest advertiser in traditional media outlets, it is increasingly difficult for newspapers to resist potential "covert censorship" that may come with withholding of advertising revenue.

Surveillance also means internet and social media monitoring. The UK-based non-profit Privacy International (PI) has reported that Safaricom, Kenya's leading mobile internet provider, allegedly provides information to government authorities, allowing for the interception of both meta-data and content.[48]As indicated by Freedom House, the government "periodically polices the internet for content that is

perceived to be morally objectionable," and "has increasingly sought to have content removed online" and from social media profiles.[49]

The technologies that allow companies or governments to monitor social media networking sites create potential for misuse, targeting certain people and groups in society, including Human Rights Defenders and journalists. For example, in a survey of Human Rights Defenders conducted by the National Coalition of Human Rights Defenders of Kenya, a "[m]ajority of respondents reported that they have experienced security breaches that include unlawful access to their social media and email accounts as well as phone tapping."[50]

Surveillance in Kenya is also slowly integrating AI data-optimization technologies, including facial recognition systems, smart policing tools, and the establishment of "safe city" platforms. The leading vendors of these systems globally are Chinese firms, led by Huawei, which has supplied these technologies to Kenya, among a larger group of about 50 states worldwide. In Nairobi, for instance, Huawei has helped install video systems that deployed 1,800 HD cameras and 200 HD traffic surveillance systems.[51]

By following China's lead in harnessing AI, facial recognition and biometrics technologies for social control, governments in Kenya, Nigeria, South Africa and other African nations could be using algorithmic, CCTV cameras[52] and digital ID systems to intimidate and coerce critics of the state. Last year, the US-based think tank Freedom House claimed Beijing was training African states on some of its own restrictive online measures.[53]

**Dynamics of Power and Resource Capture** - In Kenya, established political and economic elites have used the business of winning elections to consolidate existing dynamics of power- and wealth-capture. While the country, in particular its youth, needs critical investments to have a chance of participating more equally in the digital economy, the business of spreading "emotion wars" is paid in bills of several millions. Between December 2015 and April 2016, the Jubilee party paid the SCL Group $1.25 million and the full budget of the influence work done by Cambridge Analytica and SCL in 2016 amounts to about $6 million.[54]

> By influencing global norms and technical standards, China's diplomatic efforts at the UN increasingly aim to defend a form of cyber-nationalism.

The story of "emotion wars" goes beyond the data-predation organised by opportunistic foreign corporations. Elections are also increasingly turning into a referendum on the governance model that will shape Kenya's digital economy. For a foreign tech-leading nation like China, which is heavily investing in Kenya's digital economy, the rush towards digitization presents new opportunities to engage into sophisticated normative influence campaigns.

By influencing global norms and technical standards, China's diplomatic efforts at the UN increasingly aim to defend a form of cyber-nationalism that normalizes pervasive digital surveillance and new forms of political and social control.[55] Concretely, on the ground, through the technical infrastructure of Nairobi's new smart city, China is also slowly influencing the governance model of Kenya's digital future. What is at stake, beyond scientific collaborations, is a systematic long-term engagement by a tech-leading power to build and control the digital roads and bridges of cyberspace.

The next section will unveil what this report calls Africa's rising "Internet of Bodies and Minds," the transnational information infrastructures that make it possible for public and private actors to monitor the "digital bodies and minds" of populations in several African digital economies. In the context of elections, exploiting populations' data and controlling information networks lead to precise forms of political and behavioural engineering. It also turns powerful systems of "digital rumours" into alternate info-spheres that can be used to manufacture and spread "emotion wars." The rationale behind this section is to understand how state and foreign actors, public authorities and private corporations, exploit new disinformation architectures.

# MATRIX – THE ANATOMY OF INFORMATION DISORDERS

| INFORMATION DISORDERS | MANUFACTURING & SPREADING EMOTION WARS |
|---|---|
| | **Current Techniques & Strategies** |
| *Population-data exploitation* | 1) building voters' profiles using leaked, sold or un-encrypted data from large government and private services databases; |
| *Online Hate Speech, Virtual/Graphic Ethnic Polarisation* | 2) crafting vivid, even graphically violent propaganda that exploit ethnic and socio-economic tensions to target segments of the electorate defined by ethnicity, political leanings and age; |
| *Anonymous, Automated-Texting Campaign, "Attention by stealth"* | 3) relying on networks of political campaign surrogates to inundate information spheres, including private messaging applications (WhatsApp and Telegram Channels), TV/radio, and social media |
| *Engineered Virality* | 4) relying on botnets for viral propagation; running powerful digital ad campaigns and tweaking algorithmic search engine and algorithmic content-regulation on social media platforms; |
| *Eroding Virtual Civic Space and Social Fabrics* | 5) silencing resistance by repressing traditional media structures and harming the reputation of knowledge-institutions (for ex, EMBs) |
| *- Precision Emotional & Behavioural Engineering*<br>*- Rumours Replace Virtual Civic Spaces and Erode Social Fabrics* | 6) a powerful system of digital rumours turns into alternate infospheres, a self-evolving machine of deception, channelled both by the word of mouth and privatized, encrypted media. Digital Rumours become part of the trusted social fabrics, yet feed on inflaming economic and racial tensions. |
| | **AI-driven Techniques & Strategies** |
| *Precision Biometrics Manipulation & Attacks* | - Automated Data-Synthesis: Impersonations and Forgeries, including audio-spoofing, Deepfakes, false speeches/news articles generated by algorithms |
| *Mobilization of larger population subgroups around violent narratives*<br>*> The Menace of Unreality* | - Automated Data-Poisoning: Poisoning data in critical information infrastructure, for instance related to biometrics civic & electoral registries<br>- Automated Behavioural-Engineering: facial and affect-recognition help algorithms and their automated mercenaries (botnets) accelerate and scale emotional and behavioural engineering of larger audiences |
| **INFORMATION & CYBER-OPERATIONS** | Data-poisoning or cyberattacks targeted at electoral, political and scientific information infrastructure |

| | |
|---|---|
| **SURVEILLANCE APPARATUS** | Social Media and Internet Monitoring: computer interference (FinSpy), mobile device hacking, network surveillance, international mobile subscriber identity-catchers, deep packet inspection tools<br><br>Safe Cities: CCTV cameras; algorithmic software detecting abnormal behaviour and analysing human actions for forensics investigation<br><br>Biometrics Assemblage: Facial and body recognition tools; Biometrics and bio-data analysis (voice, iris, fingerprints, lobe and palm geometry, gait, palm's vein flow, sweat, heart-beat, pupil dilatation, DNA); Affect recognition and neuro-synchrony: when, across sub-populations, videos elicit strong emotions and electrify attention (cf. virtual violence, online hate speech, deepfakes) |
| **POWER & RESOURCE CAPTURE** | - Domestic digital manipulation of populations for ascertaining privileges and regime stability, resource and media capture<br><br>- Interference by foreign powers: interfere directly with a targeted nation's political & electoral processes, undermine populations' trust and resilience, for resource capture and territorial/geostrategic positioning |
| **DIGITAL AUTHORITARIANISM** | - Normalizing methods which serve a securitisation agenda and regime stability, including surveillance, control and repression; Limits on political agency; Infringements on Human Rights |
| **CYBER-SOVEREIGNTY MODEL** | - Technical and normative standard-setting for control over transnational information infrastructure<br><br>- Data localisation, and increasingly, regulating corporate data flows, storage, and protection with the goal to tighten grasp on growing private sector data |
| **GEOPOLITICAL IMPLICATIONS & CONVERGING THREATS** | - Multipolar competition, yet increased digital interdependence and tech convergence; significant impacts of converging technological threats<br><br>- Lacking normative and technological leadership on shared problems (pandemics, climate-change for which global data-sharing is crucial)<br><br>- Disempowerment of populations and rising human insecurity |


© iStock/Monsitj

# AFRICA'S INTERNET OF BODIES AND MINDS

Across Africa, societies are about to face an unprecedented transformation powered by the integration of AI and data-optimization technologies into politics, daily life and elections. Since spring 2019, nearly 40 million Kenyans had their fingerprints and faces scanned by a new biometric ID system that will play a crucial role in the next 2022 election.[56]

> "Across Africa, societies are about to face an unprecedented transformation powered by the integration of AI and data-optimization technologies into politics, daily life and elections.

To be eligible for essential public services from healthcare, food allowance, welfare to apply for employment and internet access, individuals in Kenya, Nigeria, South-Africa, Tanzania, Uganda, Ghana or Somaliland[57] need to register their fingerprints, facial and iris scans (Map 2). As eloquently coined by Shafi Ali, the head of the Nubian Rights Forum, who has studied the implications of biometrics ID on the ground in Kenya, not having a digital ID makes you "a living dead."[58]

In February 2019, the French company, Gemalto, announced a smart-policing collaboration with the Uganda Police Force to deploy both, Cogent Automated Biometric Identification System and LiveScan technology.[59] With the software LiveScan, police forces can capture individuals' biometrics that algorithms will help connect to mugshots and personal information. The Ugandan police will also pioneer the use of portable biometric identification devices that can confirm a match on the spot. Converging technologies are making "digital bodies" legible in real-time.

Implications for populations' privacy and agency could be corrosive. State and private sector actors engaged in shaping the political regimes of African nations could exploit the combination of AI and populations' sensitive information to exert new forms of political, social and behavioural engineering. Equipped with the technological tools to analyse and control how humans act upon information and knowledge, government and corporations involved in Africa's elections can increasingly monitor and influence populations' attitudes with the drastic potential to manipulate and restrict political agency.

Digital ID systems aim to realize the promises of the digital economy, bringing prosperity through e-finance services, fostering inclusion and empowerment through fair and free elections. These promises will be achieved if governments can operationalize an appropriate and comprehensive regulatory framework that protects personal data and safeguards minorities from marginalization. Under logics of solutionism and securitization, biometric, algorithmic and digital ID networks may already codify discrimination and gradually lead to surveillance and the monetization of personal information.[60] Most troubling perhaps are gaps in accountability and responsibility for risks, in particular when those technologies are used in elections.

> "Most troubling perhaps are gaps in accountability and responsibility for risks, in particular when those technologies are used in elections.

## Precision Political and Behavioural Engineering

What is radically different in the current age of technological convergence is the increasing capacity for state and non-state actors to analyse, predict and seek to influence – in real-time – how a target population knows, thinks or feels about the world


© UN Photo/Albert González Farran

around it. This emerging capacity is born out of the convergence between AI and technologies that capture the sensitive data of our inner lives—our biometrics and consumption patterns, our emotions and conversations, our thoughts and choices.

The AI industry posits that algorithms, deployed on globalized digital networks, can learn to map, measure and classify populations' behaviours, and, to some extent, their affective and cognitive functions. For instance, the company Kairos sells to the retail industry video-analytics cameras that correlate clients' demographic profiles with a set of predefined emotions.[61] And it is not just the industry. MIT Media Lab explores methods for nudging individuals towards well-being, parsing through their physiological, mobile phone and behavioural data.[62]

Invading the lucrative business of elections, most data-broker companies and political data consultants now also acquire baseline data about voters' affective and cognitive responses to political information, with the ultimate goal to learn how to manipulate political agency.[63] As the U.S. 2016 presidential election race was getting to an end, the Trump campaign allegedly spread online propaganda to de-mobilize black voters in Florida by attributing racial comments to Hilary Clinton.[64] In the Philippines, sophisticated teams of PR strategists, social-media influencers and bots manufactured powerful rumours about a drug crimes' epidemics, supporting Rodrigo Duterte's campaign.[65]

This trend towards "precision political and behavioural engineering" is likely to accelerate at the same rate that large technological platforms commodify data about citizens across the world. For instance, ZimGo Polling, a South Korean company that operates in the US and beyond, relies on both, natural language processing and automated affect-recognition, to analyse how citizens feel about real-time issues.[66] The US-based firm HaystaqDNA provides political parties with quantitative and qualitative

> This trend towards "precision political and behavioural engineering" is likely to accelerate at the same rate that large technological platforms commodify data about citizens across the world.

analysis of how individual voters react to a selective list of political issues.[67] As explained in a report from Tactical Tech, these include the latest hot-button issues such as "presidential approval and immigration policy, support for activist groups and movements such as Black Lives Matter, as well as consumer habits such as being a rideshare user."[68]

Every day, we transport in our pocket a window into strategic aspects of our professions, our interests and our most intimate thoughts. In most countries in Africa, even more, cell phones are the main interlocutors within economic and personal lives. Within digital networks, sensing technologies and personal devices keep proliferating, from facial and affect-recognition, gait analysis, digital assistants, microchipping, digital lip-reading, fingerprints, iris scans and sensors.[69] These technologies form the "Internet of bodies and minds," a data-ecosystem, in which everything about humans is captured, stored and analysed by algorithms. In South Africa, a country suffering from incisive racial and socio-economic tensions, surveillance networks are gradually expanding. Relying on AI and facial-recognition – this technological arsenal monitors populations in public space for "unusual behaviours."[70]

In truth, such behavioural monitoring is likely to come with an extensive rate of errors (false positives and negatives) and significant biases. Kate Crawford, Head of the AI Now Institute, got to the heart of it: "these tools are dangerous when they fail and harmful when they work."[71]

With its inherent biases, AI will still watch, track, and evaluate individuals, from the predictive power of one algorithm to the next. Societies may unwittingly give algorithmic networks unprecedented access to bodies and minds and create possibilities for political and social control. In this "Internet of Bodies and Minds," everyone is under personalized surveillance, in a post-modern version of Foucault's biopower.[72]

This is not a far-off future. And particularly, in a growing number of countries in the Global South, we see emerging lucrative networks of citizens' personal information, from social media conversations, financial banking transactions, biometrics and digital ID characteristics, to patterns of mobile phone usage.

> "In this "Internet of Bodies and Minds," everyone is under personalized surveillance, in a post-modern version of Foucault's biopower.

As they rush for the digital economy's promises with the backing of international donors, countries in Africa are in the process of turning fragmented, public and private population databases into a centralized smart identity ecosystem. Under a new logic of solutionism and experimentation, webs of demographic, personal, biometrics, medical, financial and consumption data of million African citizens are increasingly interconnected to determine digital profiles and create economic opportunities, but they also generate security risks.

## Across Africa: Monitoring and Controlling Digital Bodies and Minds

In section I about *The Anatomy of Information Disorders*, we define, as one prevailing trend, the increasing capacity and willingness of state and private sector actors to exfiltrate and exploit in elections sensitive data from population databases. This trend is described at more length below.

Across Africa, state and private sector actors increasingly harness the alliance of mobile networks' data and digital identification technologies for monitoring populations. Such complex ID ecosystems increasingly play a central role in the administration of elections.[73]

Political intelligence and influence materialize through access to interconnected datasets about voters. Ruling and opposition political parties, often in collaboration with firms of digital consultants and data-brokers, can exfiltrate sensitive personal data from an array of online public and private population databases for targeting socio-economic and ethnic voters' subgroups. Political and corporate campaigns can therefore exploit citizens' personal profiles and information networks for spreading targeted propaganda, hate speech, mis- and disinformation.

A complex identity ecosystem, combining populations datasets generated by governments, private sector services and internet platforms, creates opportunities for getting and buying access to citizens' demographic, ethnic, social and personal information. Layers of this identity ecosystem include civic, national ID and voter registries; private sector providers such as mobile networks providers, banks and financial services; and social media networks.[74]

*What are the **data reservoirs** that can be used to exploit voters' vulnerabilities through social engineering in elections?*

**Social Media Networks and Internet Platforms:** Population monitoring starts with the expanding of social media platforms (like Facebook and YouTube) and private messaging applications (for instance, widely used in Africa, WhatsApp and Telegram). These networks can be infiltrated and mined for sensitive data-collection about users. Such data ecosystems have increasingly been harnessed by political parties, P.R. and data-broker corporations to access and capture voters' digital phenotypes that elicit information about political leanings, social and ethnic backgrounds.

**Government and National ID Civic Registries:** Government registries are curated by different public agencies or centralised by the state with the purpose of recording and verifying the identity of citizens as they are eligible for an array of public, social and welfare services.

Kenya's complex digitization and integration of public services databases create further opportunities for getting access to citizens' demographic, social and personal information. The e-Citizen platform, which centralizes most of Kenyans national ID profiles, does not encrypt its datasets, making it possible for the ruling political party to have access to personal data that may be used for political manipulation operations.[75] Such platform can provide precise insights into an individual's ethnic background, political orientation, education level, wealth, dependants, residence and mobile phone number.

In 2006, Nigeria terminated a former phase of its national effort to build up a citizen registry with SAGEM, a French technology vendor, for contract breach and bribery of officials. However, at that point

> "Political and corporate campaigns can exploit citizens' personal profiles and information networks for spreading targeted propaganda, hate speech, mis- and disinformation.

the company had collected the personal information of 35 million Nigerians.[76] SAGEM' status as a foreign company prevented the Nigerian government from exerting meaningful control over its data-use after termination.

Digital ID systems give state, public agencies, technological vendors and private sector actors access to citizens' sensitive information – their "digital bodies – which can become the object of additional forms of political and social control. In Malaysia, the government's digital ID and biometrics platform facilitates intergovernmental data-sharing but falls short when it comes to data-security. Malaysia has been involved in several data-breaches, among which the large amount of customers' personal information exfiltrated from telecommunication and mobile service providers.[77] In 2016, hackers stole the personal data of over 200,000 Malaysian organ donors to create fraudulent identities.[78]

In his description of Cambridge Analytica data-mining operations, whistle-blower Christopher Wylie revealed how the government of Trinidad and Tobago leaked to the firm massive amounts of citizens information, including IP address, location and demographic profile. The data files were precise and sensitive enough to allow Cambridge Analytica to hack voters' laptops.[79]

**Biometrics or Traditional ID Voter registries:** Depending on national structures, official voter registers may be administered at the state or local level and they traditionally consist of a combination of voters' names, date of birth and current residence. Yet, in several countries in Africa, voter registers contain additional personal information, including ethnicity and increasingly biometric data. Often, election staff, political parties, candidates and holders of elected office can legally access or buy these datasets for "electoral purposes."

At the time of the 2017 elections, Kenya was already registering voters using a combination of traditional ID profiles with biometrics data.[80] In 2018, media reporting found that staff members at Kenya's Independent Electoral and Boundaries Commission who were mandated to protect voter profiles made millions of Kenyan shillings by illegally selling private voters' data to politicians during the 2017 general election.[81] In a 2018 report form Strathmore University's Centre for Intellectual Property and Information Technology (CIPIT), Kenyan expert, Robert Muthuri, explains how both major campaigning parties gained access to personal voters' data to target them with large amounts of unsolicited political text-messages: "We posit that the data-involved in such mining involved voter registration data, particularly, the names and addresses of potential targets. In Kenya, such targeting is easier because peoples' names show their ethnic background."[82] Voters' registration information was subsequently connected to social media profiles and mobile phone numbers to achieve more precise targeting within personal networks. While raising concerns over the near- and long-term security of biometric data, the CIPIT report suggests that only alphanumeric data, not biometric data, were used in micro-targeting to increase voter-registration and voter-turnout.[83]

Zimbabwe provides another troubling example when it comes to exploiting personal information from population subgroups in the context of elections. Zimbabwe's Electoral Commission had planned to use biometric voting ahead of the 2018 general election, but subsequently announced that biometrics would only be used for voter registration and not for verifying voters' identity on polling day. Yet, on the day after the 2018 elections, agents of Zimbabwe's ruling party organised a systematic campaign requiring some voters to provide their biometric registration slip serial numbers. Report from the community advocacy group, Kubatana, alleges that "ruling party agents had instructed some voters to submit the serial numbers on their registration slips along with their ID numbers — so that the ruling party could ascertain who they had voted for."[84]

It is worth noting that data-exfiltration or leaks from electoral databases are pervasive, taking pace across the globe. In February 2020, a security vulnerability was detected in an election mobile application used by Prime Minister Benjamin Netanyahu's party to communicate with voters. The software flaw exposed the government's entire voter registry, the personal data of every eligible voter in Israel, including full names, addresses and identity card numbers for 6.5 million people.[85] Three weeks before voting time, the risk was high for potential electoral manipulation and identity theft.

In 2016, a cyberattack targeted the Philippine Commission on Elections and led to the transfer of the full 340-gigabyte database of 55 million registered voters to another website. The data exfiltration encompassed names, dates of birth, addresses, email-addresses, parents' full names and, in some cases, passport details and identifiers of fingerprints.[86] This trove of data was leaked online, allegedly by Anonymous Philippines and LulzSec Philippines.

In 2018, the Indian government biometrics database, Aadhaar, was the target of multiple cyberattacks that potentially compromised the ID profiles of large swaths of the 1.1 billion registered citizens.[87] Until intervention by the Indian Supreme Court to prevent commercial surveillance, any private entity was allowed to use the state's biometric ID infrastructure for authentication, including banks, telcom companies, and a range of other private vendors with little scrutiny or privacy safeguards.

Troubling implications for privacy and data security do not seem to deter governments from promoting similar centralized biometric ID system elsewhere. In Brazil in October 2019, a week before a government's decree was signed to launch a new centralized biometrics ID database, 92 million personal records were leaked, allegedly from an existing Brazilian government department and auctioned on the dark web.[88]

**Private Services Databases:** In the Internet of bodies and minds, bits of data about a person are spread out, both in the hands of government entities and countless private companies. As a result, the risk of data leaks leading to social engineering lies

> In the Internet of bodies and minds, bits of data about a person are spread out, both in the hands of government entities and countless private companies.

within not simply the breach of, say, a government database of voter files, as was accomplished during the 2017 Kenyan election. Private companies' data can also be exploited for social engineering by data-brokers and political parties. For instance, even hacking a user list of a particular company would lead to insights about those customers buying habits, and could even speak to preferences that could highly correlate to their likely party affiliation. In this way, the cumulative effect of data breaches from a number of companies could shed powerful insights on many citizens. For some countries such as South Africa that have experienced numerous data leaks affecting over a million citizens in the past few years, parties looking to capitalize on social engineering won't have to look far beyond the data already being leaked to learn about how to manipulate the emotions of the voter base.

In 2017, personal information of 60 million South Africans was leaked from the real-estate company, Jigsaw Holdings.[89] The same year, millions of citizens' identity numbers were leaked online from Dracore, a consumer database, along with consumers' gender, ethnicity and home ownership.[90] In 2020, the GPS company, Garmin South Africa, felt victim of a cyberattack that exfiltrated South Africans personal and full credit card information.[91] Tactical Tech reports how "a data-breach at a leading South African company resulted in the loss of personally identifiable information for an estimated 31 million people, including the President, finance minister, and the Minister of Police; the data included income, address and phone numbers."[92] Research from the US' Ponemon Institute assesses that a data breach costs South African companies on average $3.06 million – nearly R50 million.[93]

Private service providers, such as banks and mobile network operators, are an integral layer of Kenya's complex identity ecosystem, as they are increasingly required to record users' personal information (such as names, birth dates, income, address and phone numbers) under security programs ("Know Your Customer").[94] While mobile network operators have taken minimal measures to anonymise customers' data, recent research suggests that these operators share their databases with bulk SMS providers. Muthuri's research shows that content service providers disregarded national guidelines and allowed targeted political messaging during the 2017 election campaign.[95]

**Compulsory SIM Card Registration:** Widespread in Africa, where 94% of mobile connections are made via prepaid plans, compulsory SIM card registration is another layer of the digital identity ecosystem. Introduced in 50 African countries as of 2019, mandatory SIM card registration laws require that people provide personal information, including a valid ID and sometimes their biometrics, before they can purchase or activate a prepaid SIM card for their mobile device.[96] (Map 3)

Such laws can allow the state to "identify the owner of a SIM card and infer who is likely to be making a call, sending a message, or making a particular financial transaction through a money transfer application."[97] Prepaid mobile phone plans are also de facto required for users to access online applications like Facebook, Twitter, YouTube and WhatsApp. Controlling and monitoring SIM card registration therefore gives authorities and private sector actors pervasive access to meta-data about citizens such as social profiles, device information, location, and search history.

By providing governments with the tools to capture, analyse, and optimize citizens' personal data far more precisely than ever before, compulsory SIM card registration amplify the power of Africa's "Internet of Bodies and Minds." As well emphasized by Privacy International, what matters is access to civic space and social services: "mobile services are increasingly becoming necessities—particularly in areas less served by other forms of information-technology infrastructure—for African populations to access education and health care information, stay informed about current events, buy and sell goods and services, participate in democracy, and stay in touch with one another."[98]

Yet, in Africa, access to this important virtual "civic space" is increasingly mediated by the state. The UN Special Rapporteur on Freedom of Expression recognized that SIM card registration policies "directly undermine anonymity, particularly for those who access the Internet only through mobile technology. Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest."[100]

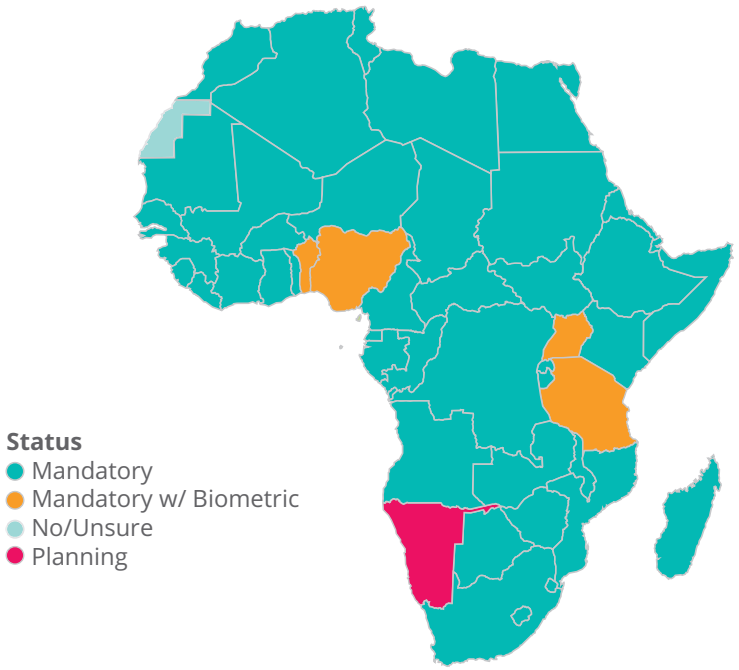
For years, nations in Africa have faced severe insecurity threats: for instance, South Africa[101] has witnessed rising criminal activities, including murders and sexual assaults, while Kenya[102] has suffered violent terrorist attacks by the terrorist group Al-Shabaab. To preserve national security and fight crime, both countries have been applying mandatory regimes for SIM card registration based on demographic, social, personal and ID information. Such centralized, mandatory registration schemes provide powerful, widespread forms of information control in Kenya, where over 99% internet connectivity is through mobile services, with over 70% being provided by one mobile network operator, Safaricom. Monitoring the identity of those who use mobile phones also means controlling access to the country's active social media scene. In 2017, private messaging platforms such as WhatsApp had the highest number of users estimated at 12 million per month, followed by Facebook at 7.1 million and YouTube at 8 million.[103]

In **Nigeria**, since 2011, regulation imposes mobile phone service providers to capture and register biometrics (facial scans and fingerprints) and personal information of subscribers in a centralized database maintained by the National Communications Commission. Privacy International reports that "in October 2016, the NCC imposed a $5.2 billion fine on a major operator for its failure to disconnect 5.1 million unregistered SIMs."[104]

Other countries in the Global South are potentially vulnerable to new forms of control over information networks. In Myanmar, a country lacking robust privacy and data protection laws and where minorities are subject to exactions and persecutions, the government is considering a national plan to capture the biometrics, demographic and personal information of users buying a mobile SIM card.[105]

Such monitoring trends based on personal data-exfiltration have serious implications in African countries where massive human populations databases are being built. While lacking robust regulatory mechanisms to apply and translate data protection

**Map 3** | Mandatory SIM Card Registration[99]



> Access to citizens' personal information is increasingly harnessed by political parties, with the support of private sector actors, to influence segments of the electorate.

laws into operational normative mechanisms, countries such as Tanzania and Nigeria are currently planning or implementing the use of biometric identification attached to SIM cards. Kenya's recently paused plans for a national ID system which would connect digital identification information with GPS coordinates and specific types of biometrics, such as "voice print" and DNA samples.[106] Kenya's high court ruled that collection of DNA and GPS data was intrusive and unnecessary and temporally deferred the biometric program until the government passes laws to ensure privacy, data-security and prevent discrimination against minorities.[107]

A strategic hotspot for security, migration control, and vital mineral resources in the Sahel, Niger is one of the latest countries to adopt biometric ID for voter registries – a contract that was signed early 2019 with French company Gemalto for an initial cost of 20 million Euros. Former Vice President of the National Electoral Commission, Mr. Kadri, one of Niger's experts in privacy law, has expressed concerns that this biometric transition is happening in a context of high regulatory fragility, as Niger's 2017 Privacy law has not been translated into operational mechanisms and lacks an enforcing authority.[108]

Attempts at social engineering in elections find powerful echoes in several African countries where access to citizens' personal information is increasingly harnessed by political parties, with the support of private sector actors, to influence segments of the electorate. The ultimate goal is to shape electoral outcomes and solidify dynamics of power and resource capture.

One hard truth is that, in African countries with recent history of racial and ethnic divisions, intensive, rapid efforts to build a centralized identity ecosystem based on sensitive populations' information (from ethnicity to social and location data) amplify ways to impose discrimination and exclusions, repression and surveillance. At least 5 million Kenyans are suffering hurdles to obtain the documents required to get a biometric ID. Kenya's biometric ID program is hurting already vulnerable populations, in particular groups from Nubian, Somali or Indian descent, reproducing entrenched inequalities and potentially exacerbating ethnic tensions.[109]

A second hard truth is that, without operational and meaningful accountability mechanisms, a centralized digital ID ecosystem could be monetized and instrumentalized by political actors for social engineering and election shaping. Digital ID databases, when correlated with mobile phone services and social media profiles, also create the potential for controlling citizens' channels of information. Depending on whom controls those spheres of information, they can be harnessed for online ethnic profiling and polarization, including targeted hate speech.

A set of factors drastically magnifies concerns over state and commercial exploitation of human populations databases. The first factor is the growth of aggregated public and personal data within the "Internet of Bodies and Minds." A second factor is the increase in the number of actors who may gain potential data-access, from government agencies, political parties to technological vendors, private sector operators and data-mining corporations. These two factors lead to the subsequent weakening of the distinction between what is considered "public" and "personal" data, raising questions about how such collection of information should be used. Finally, our societies lack a comprehensive understanding over how automated intelligent systems conduct data aggregation and analysis, with potential for built-in biases.

> Digital ID databases, when correlated with mobile phone services and social media profiles, also create the potential for controlling citizens' channels of information.

Despite increasing efforts to protect privacy, existing data-infrastructure about populations across the world have been permeable to state and commercial data-exfiltration and surveillance, including for election shaping. Public-private collaborations and normative leadership are both sorely lacking to translate newly adopted data-protection laws into operational and accountable mechanisms.

In a nutshell, the consequences of such exploitation of populations-databases and digital ID systems in elections could be corrosive. The entire history of individuals and populations – in intimate granularity, from online behaviours, dating patterns, medical records, drug consumption, sexually-transmitted diseases – could be leveraged for targeted propaganda, intimidation and discrimination. For instance, Privacy International reports that Kenya's government "has been collecting biometric information regarding people with HIV, including to determine how many people were living with HIV."[110] Such data-collection practice could amplify stigmatisation if datasets are leaked and could lead to excluding vulnerable populations from essential public services.

Governments across Africa are converting to more centralized digital identification mechanisms, which raise serious data-security, ethical and human right concerns. The risks are significant and accentuated as a result of the technological convergence behind the "Internet of Bodies and Minds." Digital bodies and minds become traceable through an array of personal devices, from laptops to cell phones that can then be targeted by automated text messages in electoral campaign operations run on WhatsApp and Twitter.

© Nairobi, Kenya/Jacek Sopotnicki

# MANUFACTURING & SPREADING EMOTION WARS

For decades, corporations in the military intelligence and political consultancy business have led intrusive data-mining operations to measure, quantify and analyse far-away populations with the goal to make them traceable and legible, like "digital bodies and minds." Scholar Simone Browne uses the term "digital epidermalization" to describe algorithmic practices that aim to monitor and control vulnerable migrant communities and marginalized populations.[111]

Increasingly, the convergence of pervasive technologies for data-capture and predictive analysis constitute a "surveillance assemblage" that intelligence firms can rely on for what they call precise monitoring and behavioural engineering. Over years, the SCL Group has extended its data-mining work across Africa, with operations spanning from Libya to Rwanda and from South Sudan and Somalia all the way to Ghana.

The data and practices exploited for behaviour change usually depended on the information needs of SCL's clients and these practices often pertained to monitoring populations' characteristics and behaviours.[112] The SCL Group built public perception profiles about nutrition and sanitation in Rwanda, healthcare issues in Ghana, instability trends in Libya, disarmament and militarized youth in South Sudan.[113]

In the near-future, as the digital economy expands across African countries, the risk arises that campaigns of corporates and external state-actors to influence behaviours will not only target voters, but decision-makers and regulators. As they weigh critical legal tensions between individuals' privacy and securitization, it is a battle of normative influence that governments in Kenya, Nigeria, South Africa and other countries are already facing now.

Political consultancy companies have made a lucrative business of breaking down populations into a number of discrete meaningful data flows that can be used during electoral campaigns for profiling, micro-targeting and, ultimately, crafting social engineering operations. Political consultants are learning rapidly from neuro-marketing techniques, which exploit the data gathered from people's digital bodies and minds to create ads and shape talking points that trigger voters' underlying psychological predispositions. For instance, Bellwether Citizen Response, a progressive consultancy, relies on facial-recognition, electro-encephalogram, galvanic-skin response, and heart rate to craft campaigns that resonates emotionally with citizens to facilitate positive change.[114]

> "As the digital economy expands across African countries, corporate and external state-actors will not only try to influence voters, but also decision-makers and regulators.

Such behavioural and neuro-marketing techniques should be assessed with high-dose of scepticism when it comes to their impact in shaping voters' perceptions and decision-making. Yet, what needs to be analysed and subsequently mitigated is the extent to which such techniques play a heavy, detrimental role in damaging political debates, amplifying polarization and, even worse, inflaming socio-economic and racial tensions within fragile societies.

New practices of biopower – aimed at social and behavioural engineering – are crafted with the financial support and complicity of ruling political elites that usually act for electoral gain as well as power and resource capture. Even when electoral impact is not proven, these practices are harmful. The risk is that established political and economic elites could keep waging online social and ethnic wars to serve their privileges of power and wealth.

Harmful ramifications come from exploiting populations' sensitive data and spheres of information. In his description of Cambridge Analytica data-mining, whistle-blower Christopher Wylie reveals how the government of Trinidad and Tobago leaked to the firm massive amounts of sensitive citizens information to help the incumbent party revamp its campaign. IP address, location and demographic identification turned those citizens' digital bodies into traceable data points to the extent that, from his computer in London, Wylie was able to spy on individuals in the Caribbean.[115] In the run up to the 2017 elections in Kenya, election officials allegedly sold voters registration data to major political parties for millions of Kenyan shillings.[117]

In Kenya, Nigeria and South Africa, campaigns to "monitor and influence the pulse" of the electorate have focused on instrumentalizing ethnic and socio-economic tensions. Such influence operations function on a reductionist notion that elements of civic debates and populations' concerns can be almost exclusively mobilized around pre-identified fears, hatred and prejudices. Such reductionism has been exposed by multiple movements of resistance, particularly in Kenya and South Africa, where civil society activists, journalist, feminists and young thought leaders used social media to organize concurrent virtual spaces for civic debates sharing insights across ethnicities.[117]

While resistance to political engineering has grown stronger, citizens, journalists and civil society activists have to organize against political parties' strategies, which increasingly capture voters' personal data, information channels and national media structures. Established governing elites, hiring – for millions – the services of political consultancies in the West, have deployed disinformation architectures that are difficult to counterbalance.

> "In Kenya, Nigeria and South Africa, campaigns to "monitor and influence the pulse" of the electorate have focused on instrumentalizing ethnic and socio-economic tensions.

> "Within disinformation architectures, automated mass-texting is becoming the strategic tool at the centre of targeted outreach by P.R. firms, political parties and their surrogates.

Most of the time, such disinformation architecture functions as follows: 1) building voters' profiles using leaked, sold or un-encrypted data from large government and private services databases; 2) crafting vivid, even graphically violent, propaganda that exploits ethnic and socio-economic tensions to target segments of the electorate defined by ethnicity, political leanings and age; 3) relying on networks of surrogates to inundate information spheres such as private messaging applications as well as TV, radio, and social media; 4) running powerful digital ad campaigns and tweaking algorithmic search engine and algorithmic content-regulation on social media platforms; 5) silencing resistance by capturing or waging a war on traditional media structures.

Within disinformation architectures, automated mass-texting is becoming the strategic tool at the centre of targeted outreach by P.R. firms, political parties and their surrogates.[118] Strategists have discovered how easier it is to wage influence campaigns by targeted, anonymous messages. Mercenary trolls and automated bots that have been mobilizing segmented audiences on Facebook are now also migrating to private messaging applications like WhatsApp. This trend in digital engineering affects and affected voters in the U.S., India, Brazil and the Philippines.[119]

Everywhere, the automation factor plays a catalyst role – the fact that bots can scale up engagement with massive audiences.  But, what matters even more is the capacity to strike the electorate's "emotional nerves." India provides a dramatic example of this new emotional and behavioural engineering that thrives on powerful rumours spread by political parties with nation-wide cyber armies. Staffers from the ruling political party, BJP, run a large WhatsApp Group, called Cyber Army 400+, where Muslim communities are often portrayed as a threat to Hindus' political and social ways of living.[120]

The consequences are fatal, vitriolic in real-life. Across India in summer 2018, manipulative messages on Facebook and WhatsApp, which are used by about 200 million people, painted Muslim groups as responsible for child abduction.[121] The hysteria led to more than 30 deaths and left many injured. The trend keeps going in West Bengal, where Rohingya refugees, who fled atrocities in Myanmar, are now demonized in violent speech that rapidly metastasizes on WhatsApp.

## KENYA'S EMOTION WARS

Kenya has suffered decades of ethnic conflicts, terrorist threats and economic inequality.

The 2013 and 2017 elections have thrown Kenya into turmoil. Corrosive online propaganda campaigns spread through mobile phone, traditional and social media networks. They were crafted to fuel distrust, ethnic and socio-economic tensions between population subgroups.[122]

Such propaganda strategies were designed with the support of foreign data-analytics companies, Cambridge Analytica and the SCL Group, for influencing voters' behaviours.[123] Yet, major political parties, the ruling Jubilee party and the opposing political group called the National Super Alliance (NASA), also deployed widespread communication tactics to target specific segments of the Kenyan population.[124]

## The File is About You: Data-Mining & Profiling

In Kenya, as in several African nations, electoral campaigns have become powerful data-mining and profiling operations. In January 2020, a new trove of documents from Cambridge Analytica and the SCL group – the Hindsight Files – revealed the extent of these two firms' involvement in Kenya's elections.[125] In 2012 and 2017, Cambridge Analytica had been collecting large amounts of data – two surveys of about 50,000 households – claiming to assess Kenyans' hopes ("jobs"), fears ("tribal violence") and "preferred information channels," in what the firm deemed to be "the largest political research project ever conducted in East Africa."[126] Such profiling operations identified young voters as an instrumental population segment to target on social media and served to rebrand President Uhuru Kenyatta's two electoral campaigns in 2013 and 2017. Kenyatta came to power in 2013 and won a second term in August 2017, defeating his opponent Raila Odinga by 1.4 million votes.

> "Data-brokers have made a business of identifying individuals' deepest fears and prejudices to mobilize them around divisive issues, often dissolving the remaining pieces of shared social fabrics.

This form of data-predation raises critical concerns in a country that did not have, at the time of the latest election, robust mechanisms and an independent authority to enforce citizens' privacy. Given Cambridge Analytica and SCL's opaque practices, it is also difficult to assess the source and granularity of personal information that could have been gathered on Kenyan citizens within and beyond political surveys. The UK organisation, Privacy International, expressed concerns that "the potential data-gathering could be extremely intrusive, including sensitive personal data, such as a person's ethnicity."[127]

What we know is that data-analytics and PR firms have acquired the capacity to run intensive and widespread data-mining operations to define and curate the psychological profiles of millions of social media users. They take the emotional pulse of the electorate, which can then be used in political engineering campaigns for achieving electoral gain, power- and resource-capture. Companies like Cambridge Analytica and SCL have made a business of identifying individuals' deepest fears, hatreds and prejudices to mobilize them around divisive issues, or to induce voting distrust and apathy, often dissolving the remaining pieces of shared social fabrics.[128]

In the run up to elections in fragile states, the business of spreading "emotion wars" is as violent as it is lucrative, often paid in bills of several millions of US dollars. The Hindsight Files reveal that, between

> Data-analytics and PR firms have acquired the capacity to run political engineering campaigns for achieving electoral gain, power- and resource-capture.

December 2015 and April 2016, the Jubilee party paid SCL $1.25 million of a $1.3 million contract. SCL's bill for the 2017 election was, at least, $3.9 million but the final figure could be as high as $6 million.[129]

In Nigeria, the story is as old as 2007. Cambridge Analytica and the SCL Group started intervening in the political campaign prior to the 2007 Nigerian elections and were even more seriously involved in the 2015 race.[130]

Prior to the 2007 election, the SCL group advised the ruling Nigerian party to use religious leaders to suppress the vote and proposed to organize anti-election rallies with local religious figures on the day of polling in opposition strongholds. Election observers of the 2007 election in Nigeria reported incidents of ballot stuffing, theft of election materials, vote buying, underage voting, altering of official results and widespread violence.[131]

In 2015, the Nigerian elections became the background scene where data-miners from Cambridge Analytica colluded with Israeli cyber-mercenaries to try to engineer an electoral victory for incumbent President, Goodluck Jonathan. The geostrategic motive was to perpetuate existing corporate control over oil industries. However, opposition leader, Muhammadu Buhari, won the race, despite Cambridge Analytica's aggressive intimidation and communication tactics.[132]

## Crafting and Advertising Violent Propaganda

The run up to the 2017 Kenyan elections was marred by hateful speech and violent outbursts, including the death of the election official in charge of the e-voting system. Tensions on the streets was also matched online. Two powerful disinformation campaigns built on citizens' fears related to inter-ethnic violence, terrorist attacks and public health crises. A 90 second video of smoke and chaos with armed groups marching over cities and slums went viral on Kenya's social media networks, providing viewers with a dystopian look of what the country should expect if Raila Odinga, Kenya's leading opposition candidate, were to win the elections and establish a violent dictatorship. And with this video, traced back to a PR firm in Texas, and unleashed by search-optimizing algorithms on the networks, there was a feeling that Kenyan politics had entered the post-truth era.

Powerful video shots about armed terrorists, spiralling disease and famine were not chosen by accident. They were a virtual echo of Kenya's recent history of ethnic violence. The video was part of a dual campaign, featuring "The Real Raila," a virulent attack campaign against opposition leader, Raila Odinga, and "Uhuru for Us", a website promoting President Uhuru Kenyatta's achievements. The two online campaigns were produced by Harris Media LLC, a far-right digital advertising company based in Texas, which serves political clients, including the Trump campaign and several far-right European parties.[133]

> In the run up to elections in fragile states, the business of spreading "emotion wars" is as violent as it is lucrative, often paid in bills of several millions of US dollars.

Similar techniques of virtual, graphic violence had been tested by Cambridge Analytica and the SLC Group, in Nigeria, in the run up to the 2015 elections. Scenes of people murdered, macheted to death, were unfurling in a 99 second video made to depict Nigeria's future if the opposition leader, Muhammadu Buhari, a Muslim from the North, were to establish "Sharia for all." Terror turned into tactics to engineer voter suppression among Buhari's potential supporters.[134]

During the 2016 local elections, South Africans also became targets of political engineering tailored to

> In the run up to the 2017 Kenyan elections two powerful disinformation campaigns built on citizens' fears related to inter-ethnic violence, terrorist attacks and public health crises.

feed on the economic and social scars deepened by lasting inequality in the wake of the apartheid. The country's governing party, the African National Congress (ANC), spent R50 million to deploy its own "war room" and sow disinformation.[135] Tactics were rather old-school, from propaganda on billboards and radio shows, to pamphlets delivered door-to-door. But the ANC also imposed tight control on the state broadcaster, which is a critical medium to reach millions of voters in rural areas and in vernacular languages.

Domestic efforts were seconded by the services of another P.R. firm, Bell Pottinger, which inundated South Africa's electorate with toxic, vitriolic narratives that revived chronic racial divides. Escalating tensions against "white monopoly capital," fuelling online discourses on "economic apartheid" was the new P.R. strategy to divert popular attention from state corruption and wealth-capture by corporate barons, the Gupta brothers. Bell Pottinger helped generate hate-filled speeches and offensive cartoons – showing emaciated black beggars starving at the feet of fat, rich-looking white people gorging on food – which inundated social media, messaging apps and TV networks.[136] Violence against journalists worsened, race relations deteriorated in a setback that would weaken South Africa once again.

Like Cambridge Analytica, Harris Media builds psychometric profiles of social media users to target their emotions with more precision. To inundate WhatsApp and other social networks while also reaching specific population segments, the digital media company uses both, targeted advertising and Google AdWords. Buying advertisement on Facebook allows a company like Harris Media to identify and target population subgroups that could be highly influential if mobilised. The second communication tactic consists in making campaign websites more visible through search-engine optimization, a process in which websites are tagged with highly searched terms – in this case election-related terms – so that they eclipse other search results.

Micro-targeting segments of the population was the most efficient way to appeal to the socio-economic preoccupations of young Kenyans, but also specific ethnic groups whose votes could be suppressed by fears, or mobilized for the ruling party. Techniques of population profiling, segmentation and microtargeting inexorably destroys the common space left for pluralistic debates, strengthening political and ethnic polarization over shared social fabrics.

Harris Media's campaigns flooded an array of social and private networks – Facebook and Twitter, but even more WhatsApp and Telegram – in a context of pervasive media capture and intimidation. The campaigns' virtual cruelty mirrored real-world violence, such as the murder of a senior electoral official and accusations of hate speech by both political parties. It also reflected a war on the press, with Kenyatta's ruling party controlling most of the domestic media landscape, including the allocation of advertisement dividends.

> Techniques of population profiling, segmentation and microtargeting inexorably destroys the common space left for pluralistic debates, strengthening political and ethnic polarization over shared social fabrics.

## Disinformation Architecture

In the run up to the 2017 elections, WhatsApp groups, including non-political ones, were inundated with the two incendiary Harris Media's campaigns, as well as other expressions of rampant ethno-nationalist rhetoric, mis- and disinformation. A significant number of social media groups already existed or were formed along perceived ethnic voting blocs.[137] Micro-targeted propaganda therefore relied on assuming users' political leanings based

on their names and ethnicity. For instance, members of a certain ethnic group would receive propaganda threatening to annihilate their tribes, producing fear of mobilization and voters' suppression.

Beyond mining social media profiles, micro-targeting also relies on the exploitation of populations' databases. Recent research by Kenyan scholars point to several plausible sources of population and personal data that have allegedly been mined in the course of the 2017 elections.

In 2018, media reporting found that private voters' data were sold illegally to political campaigns during the 2017 general election.[138] In a 2018 a report form Strathmore University's Centre for Intellectual Property and Information Technology (CIPIT), Kenyan expert, Robert Muthuri, explains how both major campaigning parties gained access to personal voters' data to target them with large amounts of unsolicited political text-messages: "We posit that the data-involved in such mining involved voter registration data, particularly, the names and addresses of potential targets. In Kenya, such targeting is easier because peoples' names show their ethnic background." Voters' registration information was subsequently connected to social media profiles and mobile phone numbers to achieve more precise targeting within personal networks. While mobile network operators have taken minimal measures to anonymise customers' data, recent research suggests that these operators share their databases with bulk SMS providers. Muthuri's research shows that content service providers disregarded national guidelines and allowed targeted political messaging during the 2017 election campaign.[139]

Months before the 2017 August elections, political campaigns deployed a sophisticated dissemination architecture, encouraging supporters to organize in groups on WhatsApp and Telegram channels, integrate progressively larger audiences, and send wide automated messaging campaigns, often unsolicited and without voters' consent. Even, Kenyan political candidates were active on social media, having their staff contact large group of voters, in particular youth, on private messaging apps. In this way, also political campaigns are getting increasingly personalized.

The political campaigns behind the two main candidates, Kenyatta and Odinga, also moved their focus from analogue methods – billboards, radio, TV and newspaper advertisement – to more precise and targeted digital channels of information, such as shows on Facebook live, and discussion groups on WhatsApp, Telegram and Twitter. Through storms of

> "Beyond mining social media profiles, micro-targeting also relies on the exploitation of populations' databases.

© Unsplash/Muhammadtaha Ibrahim Ma'aji

> As the elections approached, WhatsApp groups became incubators for information disorders.

hashtags and memes, discussions turned increasingly polarized, marginalizing moderate voices. Political campaigns also hired the services of well-known journalists, religious figures and social media influencers who were used to capture socio-cultural trends, from sermons to songs, story-telling and sarcasms.

Online campaigns also instrumentalised the role of the Independent Electoral and Boundaries Commission (IEBC), leaking screenshots of meeting' minutes, internal memos, and private conversations between election officials, all spread widely on WhatsApp groups. Such tactics achieved both aims: it harmed the IEBC's legitimacy and independence, and created a form of dependence towards executive political figures.

As the elections approached, WhatsApp groups became incubators for information disorders. Research describes the multiple forms of mis- and disinformation: "impersonating legitimate news outlets, fake breaking news, leaked communications from state institutions, cherry picked and distorted facts from real news, fake screenshots of private communications, fake communication from institutions, pictures from old events with captions of current events, negative campaigning involving family and personal ties, use of parody accounts and campaigns against institutions."[140]

In a vicious circle, elements of mis- and disinformation that started first spreading on social media, found a second life offline on traditional radio and TV broadcasts, escaping any fact-checking and reaching an ever-expanding audience. This biology of disinformation leads to the power of digital rumours.

## The Power of Digital Rumours as Alternate Infospheres

In the Internet of Bodies and Minds, cell phones are powerful devices to monitor the electorate's pulse. They also become a vital personalized channel and node in a wider sensing network of trusted peers – and this is where digital rumours thrive as a renewed mode of producing and vetting knowledge about elections.

As witnessed in Kenya, South Africa, Nigeria, Brazil and India, powerful disinformation campaigns are increasingly waged over messaging apps, where interactions consist of encrypted personal conversations and "peer groups," made of friends, family and business partners. These messaging apps come in pre-paid mobile-internet plans and therefore become an accessible information ecosystem, siloed from other parts of the Internet. They become new privatized, segmented echo chambers.

Relying on private users' networks is increasingly a strategy used by political campaigns in the West. The Trump campaign is currently investing in new "peer-to-peer" texting apps that could allow a single volunteer to send hundreds of messages an hour directly to millions of voters' phones without their permission.[141] From Washington to Nairobi to Johannesburg, there is a race for political campaigns, data-brokers, P.R. and intelligence firms to access voters' cell phone numbers.

Opportunistic political actors keep discovering how easy it is to wage an untraceable "WhatsApp warfare" or capture citizens' attention by stealth, with automated anonymous text-messages. In essence, the opacity of encrypted networks recreates separated ecosystems, which are not submitted to fact-checking and policing, and where political information relies on powerful rumours in a trusted, peer-to-peer environment. Each of these ecosystems relies on a combined pyramid and network strategy in which producers create malicious content and broadcast it to regional and local activists. And sometimes, in an absurd feedback loop or vicious circle, malicious content comes back on the media scene, picked up by traditional newspapers.

As explained by experts, Hezron Ndunde and Francis Nyamnjoh, this is the return of "rumours" as an alternative way for citizens to source knowledge, learn about politics and stir mobilization. In the aftermath of the December 2007 to March 2008 post violence, scholar Hezron Ndunde analysed how the Kenyan population would recreate information spheres in a context of heightened insecurity, repression and censorship.[142] The Kenyan government had imposed

© UN Photo/Harandane Dicko

> The rationale behind this new disinformation architecture is to immerse citizens in an alternative, virtual reality where they themselves become producers of digital manipulation.

a ban on live coverage of radio and major private TV broadcasts. It also requested leading telecom companies, such as Safaricom, (p 2) to "warn the information starved citizens to desist from sending messages that were likely to perpetuate violence and hostility that had been brought about by a disputed election."[143] Against this background, Kenyans increasingly turned cell phones and the social media window they offered into a new medium for "rumours" as a form of political debate and critique.

Yet, Ndunde's research also led to a sober diagnosis that the Kenyan population's reliance on rumour for political discussion plaid a sinister role in the 2007/2008 violent exactions. His research shows how, in the run up to Kenya's 2007 elections, supporters of incumbent President Kibaki would spread text messages to warn against the power ascension of opposition leader, Raila Odinga. In some instances, the opposition leader was pictured as a "terminator" who "did not have what it takes to deliver Kenyans to the Promised Land."[144] During the 2007 Kenyan elections, online incitement to violence turned into coordinated assaults on specific ethnic groups for fictional massacres and expropriation allegedly perpetrated thousand miles away.

Ten years later, during the 2017 electoral campaigns, a short film of graphic violence, which portrayed Raila Odinga as the "Lord of War" and "Lord of Poverty," metastasized through networks of Facebook and WhatsApp's users.

The risk is that such a system of political rumours becomes a self-evolving, endogenous machine of deception, channelled both by the word of mouth and privatized, encrypted media. More troubling, this form of disinformation architecture not only becomes part of the trusted social fabrics, but also feeds on inflaming existing divisive economic and racial tensions.

The rationale behind this new disinformation architecture is to immerse citizens in an alternative, virtual reality where they themselves become producers of digital manipulation. U.S. intelligence officials recently warned House lawmakers that,

> Opportunistic political actors keep discovering how easy it is to wage an untraceable "WhatsApp warfare" or capture citizens' attention by stealth, with automated anonymous text-messages.

"rather than impersonating Americans as they did in 2016, Russian operatives are working to get Americans to repeat disinformation."[145] Interestingly, this strategy muddies who is supposed to carry the burden of intent behind spreading malicious content and makes it difficult, if not impossible, for social media companies to rely on rules that prohibit "inauthentic speech." To some extent, this is already happening in the systems of political rumours we see emerging in African elections, particularly in Kenya's 2017 election.

In this isolated system where "rumours" become part of the social fabric, the social ground in which information emerges, circulates and gets vetted by peers, the risk is that the idea of truth, real-facts and authentic speech could become irrelevant. Political and social trust and truth, both, could be "discovered" and discussed strictly in privatized echo chambers, rather than through inclusive, pluralist public debates.

The antidote to rumours as a powerful disinformation channel is the engagement and resistance undertaken by traditional media, activist-journalists and civil society actors. Local and national independent media represent a crucial element of resilience and social fabrics. Yet, in numbers of countries, including Kenya, Nigeria, and South Africa, private surveillance technologies have strengthened and tightened the grip of ruling political parties over the critical role that journalists and civil society activists play in exposing hate speech, mis- and disinformation.[146]

Fearing gendered attacks and repression, budget cuts, privacy breaches and harmful allegations, reporters and human rights defenders are often struggling to expose governing authorities' ethics and accountability failures.[147] Even the perception of being watched is enough to keep many in line. A war is waged on the press through surveillance, repression and resource capture.

The troubling and violent ramifications of information disorders have spread far beyond African elections. After leading to mass-killings, rape and destruction of villages in Myanmar, anti-Rohingya hate speech and falsehoods went viral on Facebook and WhatsApp during India's 2019 national elections, with potential for future rising violence against Rohingya populations in tinderbox regions like West Bengal.

Companies such as the SCL Group and Cambridge Analytica have shown to illiberal political leaders across the world: it is getting easier to wage emotional and behavioural engineering on the electorate by relying on automated and anonymous mass texting.

In-depth psychological and ethnographic research will be needed to assess the extent to which digital manipulation and virtual violence in pictures or videos, contribute to influence voters' behaviours and shape electoral results. Yet, what research confirms is that vitriolic, divisive rhetoric is already instrumentalized by established political parties in countries where implications are high for inflaming socio-economic and ethnic polarization or degrade trust in fact-bearing institutions.[148]

In this "deception machine," it is less the sophistication and efficiency of digital and algorithmic tools that matter – at least for now – but the degradation of trust: trust in data, election technologies, emergency systems, civilian infrastructure and governing institutions. Once populations internalize the possibility that they are being manipulated – as it was the case in Kenya – distrust, electoral apathy and cynicism won over hope for pluralistic engagement. Too often, profit, lies and power trump the empowerment of populations that have been hoping to use the same digital tools for fair and free elections.

> The antidote to rumours as a powerful disinformation channel is the engagement and resistance undertaken by traditional media, activist-journalists and civil society actors.

# IV

© Unsplash/Edward Howell

# INFORMATION DISORDERS LEADING TO SURVEILLANCE

Many news reports and commentators have portrayed information disorders in African elections as foreign interference by corporations selling political intelligence. Cambridge Analytica, the SCL Group, Bell Pottinger and the likes have become poignant examples of the dark side of the algorithmic revolution with voters' data extracted or traded away as the new coal, oil or shale gas, enshrined in a modern pact for electoral gain.

Organized preying of foreign corporations on African citizens' data and livelihood to serve powerful domestic political elites is highly disturbing. Yet, it is only one facet of a larger troubling story where information disorders are exploited by illiberal domestic political leaders to establish and legitimize forms of cyber-nationalism. In addition, a cyber-sovereignty model such as promoted by China normalizes pervasive digital surveillance and new forms of political and social control. And, as AI and data-capture technologies converge to make populations' digital bodies and minds highly legible, trends towards legitimizing, in laws and governance practices, new forms of algorithmic surveillance will have harmful implications. By constantly monitoring "traceable bodies and minds," such biopolitics forces exert and amplify dynamics of exclusion and discrimination imposed on populations that are already vulnerable. The following example of China illustrates this drastically.

## China's Biopolitics Model: Automated Ethnic Profiling and Behavioural Engineering

These biopolitics trends are striking in China where the government is building and gradually centralizing the tenets of a "unified social credit system," a large matrix of interconnected databases from which machine learning tools extract for each individual a score that can be factored into decisions on jobs, loans, transportation services, medical coverage, and other services.[149] Personal, demographic, behavioural, medical, financial and consumption data of about 20 to 30 million people have now been captured and aggregated in a watch-list to determine their digital ID profiles and corresponding social and behaviour rankings.[150]

> "Biopolitics forces exert and amplify dynamics of exclusion and discrimination imposed on populations that are already vulnerable.

A few years ago, across Xinjiang region, which is home to Uighurs, a Turkic minority group, China's government started "testing facial-recognition tracking and mandating the collection of biometric data, including DNA samples, voice samples, fingerprints and iris scans, from all residents between the ages of 12 and 65."[151]

With time, Chinese authorities have now deployed, beyond the Xinjiang region, a vast system of advanced facial recognition algorithms that have been trained to associate certain skin tones and facial features with the concept of Uighur ethnicity.[152] The facial recognition technology, which is part of an ever- expanding net of surveillance cameras in public spaces, can profile Uighurs based on their biometrics and keep records of their activities for potential police interrogation. This form of profiling makes China a leader in applying AI, facial recognition and biometrics to monitor subpopulations, with the potential to experiment with and export a new type of automated racial discrimination.

Under the government plans "Skynet" and "Sharp Eyes" – metaphors for algorithmic surveillance and intelligence collection – China is gradually expanding to populated cities its technological apparatus for social control. Police departments build databases of faces and biometrics for individuals with criminal records, mental illnesses, history of drug use, and

> Chinese authorities have deployed, beyond the Xinjiang region, a vast system of advanced facial recognition algorithms trained to associate certain skin tones and facial features with the concept of Uighur ethnicity.

those who have showed resistance through activism and state critic.

CloudWalk, a start-up well known for shaming jaywalkers by exposing their face and personal information on huge billboards, is now getting into the business of analysing the behaviour of sensitive groups of people. Beyond AI and biometrics, Chinese authorities are also resorting to phone scanners[153] – or international-mobile-subscriber-identity (IMSI) catchers – following a securitization agenda that should allow them to register the identity of all internet mobile phone users in public spaces, their internet behaviour, their location, and their movement.

Such combination of surveillance techniques is increasingly presented as a security toolkit that can be exported abroad. Domestically, China's government does not shy away from displaying what we could call modern tools of biopower. The perception of surveillance has a powerful effect on populations, normalizing behaviours, self-censoring and policing public discourse.

One topic less covered by Chinese authorities is the security of the massive throve of populations' data. Online data leakage is a growing problem, even in China. Personal information and whereabouts are monetized by unscrupulous actors with access to unprotected servers and networks.[154] Beyond unofficial data-leaks, a wide ecosystem of companies and technology vendors can gain legitimate access to citizens' information centralized in the mandatory national ID system. Collusion of interests leads to state and commercial surveillance.

To have the centralized Social Credit System fully functioning in the near-future, the Chinese Communist Party (CCP) needs to integrate parallel credit scoring datasets from an array of large private holdings, such as Tencent Credit and Sesame Credit by Alibaba-subsidiary Ant Financial Services. China's government is therefore increasingly regulating corporate data protection and storage with the goal to tighten its grasp on growing private sector data.

As explained below, over thirty nations in Africa are also establishing centralized national biometric ID platforms that will generate a unique identifier for each citizen, typically serving as a link to discrete government and private sector databases. (Map 2)

Alongside citizens' data capture, the CCP has also expanded its regulatory power to social media and internet content to ensure that state-vetted governance vision and narratives around national unity and security remain dominant in China's cyberspace.[155] Since 2017, the government has extended its control over spheres of information, blocking or filtering internet traffic and suppressing "civic spaces" that were used for pluralistic debates.

> Such combination of surveillance techniques is increasingly presented as a security toolkit that can be exported abroad.

For instance, private messaging apps' providers and administrators have to comply with credit-scoring systems and store user data for six months to ensure their services align with state-sponsored censorship.[156] In Xinjiang, policing practices include the use of mobile and Internet tools, and just having WhatsApp installed on residents' phones is scored as subversive behaviour. Since 2017, Chinese authorities have mandated all Xinjiang mobile phone users to install spyware apps in order to monitor spreading of terrorist propaganda.[157]

In China, complex interconnected systems of social-credit scoring and censorship are reducing political agency, public discourse, freedom of expression and self-determination. The surveillance net normalizes and controls citizens' spheres of information, silencing dissent and amplifying vetted narratives that support CCP' supremacy over collective security, politic and economic life. China's high-tech police state imposes a modern form of biopolitics, by engi-

neering populations' docile political and social behaviours through self-regulating and shaming practices based on personal data-exploitation.

With time, China will offer to other nations an ever more precise model to control populations' spheres of information, automate ethnic profiling and discrimination, and exploit precise political and behavioural engineering in order to shape elections and, beyond, support a robust securitization agenda.

## Every Cell Phone, A Living Brain – Controlling Information Spheres

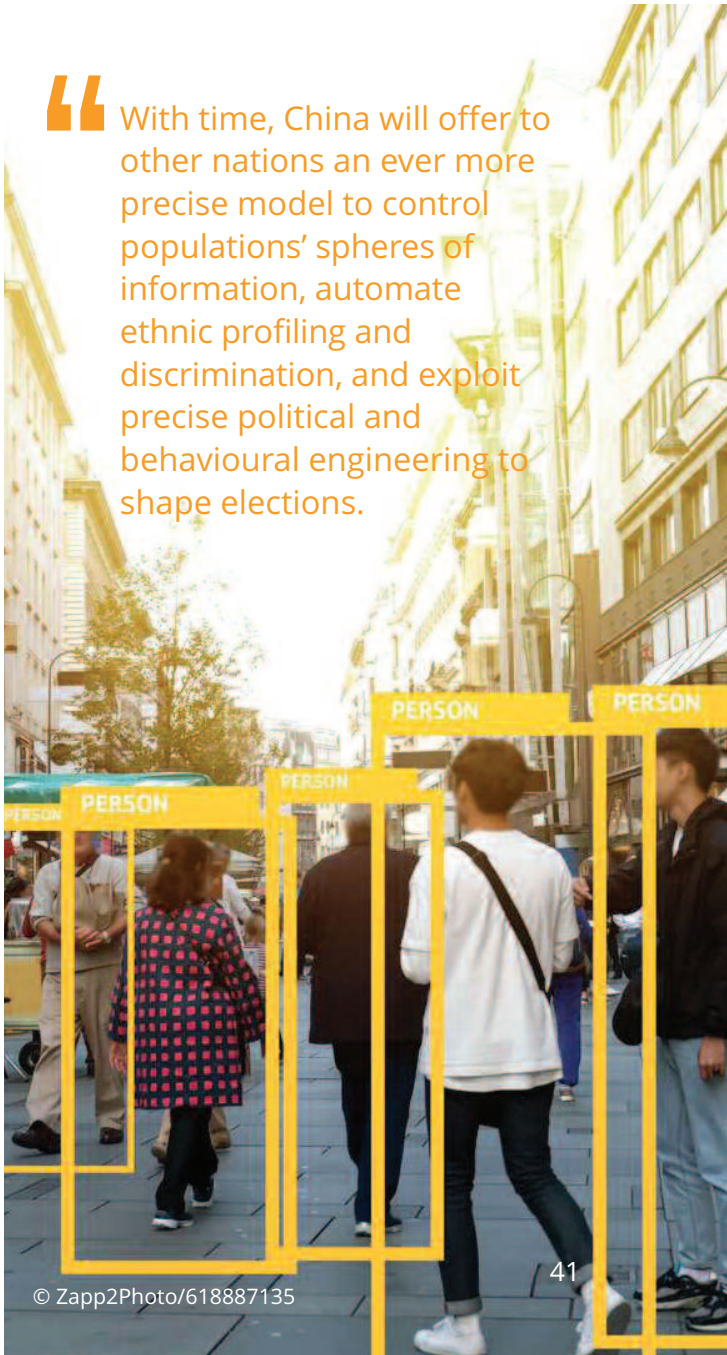
Information disorders in Kenya, Nigeria, South Africa and beyond – India, Malaysia and the Philippines are other examples – have actually well served the interest of established political elites to strengthen their securitization agenda and dynamics of resource capture. And in a vicious feedback loop, digital surveillance technologies have kept amplifying the scope of both, information manipulation and repression of those who oppose resistance.

Within the last decade, millions of people in Kenya, Nigeria and South Africa, started walking around with devices in their pocket that recorded data about everything from loans, jobs, age, likely ethnic background, political conversations, relationships, hopes and fears. Cell phones provided not only access to a national ID profile, social media and internet platforms, but a window into populations' brains with increased potential for political and behavioural engineering in elections.

With the help of data-analytics and PR companies, political parties started tapping into constellations of data networks, including civic and voters' registries, mobile network providers and private financial services to exploit sensitive data about populations. Such data-mining, profiling and micro-targeting techniques would later help craft electoral propaganda to sow polarization, violence and dissent, and ultimately favour governance models based on increased surveillance and securitization.

As the combination of AI and personal mobile devices makes digital bodies and minds ever more traceable, a growing surveillance industry sells technologies that enable governments to gain surreptitious access to the digital communications, browsing data, location history as well as online and offline activities of individuals.[158]

Beyond internet and social media monitoring, illiberal governments increasingly have access to a new class of malware that can hack individuals' computer, network or mobile devices. For instance, agents of the Ethiopian Government used the FinSpy malware to target a U.S. citizen actively involved with the Ethiopian diaspora community. According to a UN report, "FinSpy allegedly recorded the man's and his family's internet video calls, emails and other communications, including by logging his keyboard strokes, sending the data back to servers based in Ethiopia.[159]




> "With time, China will offer to other nations an ever more precise model to control populations' spheres of information, automate ethnic profiling and discrimination, and exploit precise political and behavioural engineering to shape elections.

© Zapp2Photo/618887135

> Beyond internet and social media monitoring, illiberal governments increasingly have access to a new class of malware that can hack individuals' computer, network or mobile devices.

In another series of intrusive breaches, the NSO Group's Pegasus Spyware targeted individuals' mobile devices in 45 countries, including Kenya and South Africa. Once Pegasus is installed on a cell phone, hackers can start executing arbitrary commands and exfiltrate the target's private data, including passwords, contact lists, calendar events, text messages, and live voice calls from popular mobile messaging apps. Hackers can even turn on the phone's camera and microphone to capture activity in the phone's vicinity.

Other techniques exist for governments to monitor and control online activity and communications. International Mobile Subscriber Identity Catchers can intercept communications, location and meta-data generated by personal mobile devices. Tools called Deep Packet Inspection are able to monitor, analyse, and redirect in real-time traffic passing through communications and Internet networks. Deep Packet devices can also block access to certain websites or redirect users to platforms infected with malware.

Coupled with this new spying arsenal, internet shutdowns are another radical way for governing authorities to try to control information spheres. Across the world, governments have turned to network shutdowns with increasing frequency. According to 2018 data, internet blackouts occurred in at least 11 African countries and, in India, at a rate of 134 incidents in 2018.[160] Often, authorities justify such drastic measure as a way to crush unrest and silence online hate speech and disinformation.

Not only internet shutdowns have significant negative implications for populations, empirical evidence is sorely lacking that these tactics are effective at controlling information disorders. Rumours and disinformation keep spreading through word of mouth with no virtual space for pluralistic debate and fact-checking. Acts of violence often go unreported. Economic loss is severe. In a country like Ethiopia, which has gone through a series of shutdowns between 2018 and 2019, the economic loss is about $4.5 million for every day spent offline.[161]

The government of Zimbabwe provides a poignant example of an authoritarian state regulating access to internet networks and traffic flow for shaping public discourses and controlling information spheres.[162] During the 2017/8 coup, when Zimbabwe's army deposed President Mugabe, military authorities inundated social media and broadcast channels with crafted propaganda about an open and peaceful transfer of power, encouraging populations' access to information spheres. Yet, in January 2019, after days of protest over doubling fuel prices, Zimbabwe' security forces launched a violent crackdown which led to dozen deaths and 600 arrests. The government also imposed a countrywide internet shutdown, with sustained interruption of social media and messaging services such as Facebook, WhatsApp and Twitter. Under the silence of the shutdown, security forces perpetrated more arrests, acts of torture and violence.

## In Kenya

The private surveillance industry provides governments across the world with substantial tacit knowledge, tools and strategies. Research by civil society and the UN Human Rights Council has unveiled the arsenal of surveillance tools available to growing numbers of states, including Kenya.[163]

### *Surveillance of Communications*

In 2017, the Center for Intellectual Property Information Technology Law (CIPIT) led an investigation that confirmed the presence of a "middlebox" on a Safaricom cellular network.[164] While middleboxes can be required for network optimization, they can

> Coupled with this new spying arsenal, internet shutdowns are another radical way for governing authorities to try to control information spheres.

also be used to monitor, manipulate and censor Internet traffic. Safaricom recused relying on a middlebox and subsequent tests returned negative results, leading the researchers to conclude that it was no longer in use.

Privacy International led an in-depth investigation about Kenya's practices of communication surveillance, which unveiled collusion between government agencies and mobile internet providers.[165] For instance, Safaricom, which leads the mobile internet market in Kenya, allegedly provides customers' data to authorities even in the absence of a court order. Privacy International also maintains that the Kenyan National Intelligence Service (NIS) has gained "direct access to telecommunication networks across the country, which allows it to intercept communications, including the content of the communication as well as information about who sent and received the messages, from what devices, at what time, and from what locations – without the knowledge or consent of telecommunication providers or their subscribers."[166] Privacy International's Investigation also indicated that intercepted information could be freely shared with other government agencies.

### *Social Media Monitoring*

In the months prior to the 2017 elections, Kenyan authorities have resorted to intimidation and violence

> "The private surveillance industry provides governments across the world with substantial tacit knowledge, tools and strategies.

against social media influencers and internet activists in retaliation for their online activities. Freedom House reports that "during the election period, authorities often destroyed the cameras and phones of journalists to suppress reporting on violence and human rights violations."[167] Practices of intimidation and harassment were also rampant online with frequent instances of cyberbullying aimed at female journalists and activists. Freedom House reports that, in 2019, Mombasa's police forces arrested social media users that were accused of warning others against registering for the new biometric ID system.

## In Nigeria

The February 2019 presidential election period recorded an increase in violence, harassment, and prosecutions of journalists, despite vibrant movements of online resistance.[168] Progress towards the protection of digital rights, through the Digital Rights and Freedom Bill, was halted in 2019 when President Buhari declined to sign the bill into law.[169]

> "Within the last decade, millions of people in Kenya, Nigeria and South Africa, started walking around with devices in their pocket that recorded data about everything from loans, jobs, age, ethnic background, political conversations, relationships, hopes and fears.

© Nairobi, Kenya/Nina R.

### *Surveillance of Communications*

Nigerian intelligence and security authorities often claim that a robust surveillance apparatus is justified by the fight waged against the Boko Haram terrorist group. Substantial amounts of the federal budget keep being allocated to new surveillance technology programs, including potential development of "social media mining," surveillance drones equipped with IMSI payload capabilities, and mobile surveillance facilities.

In recent years, the government has already deployed sophisticated techniques for surveillance of large swaths of the Nigerian population. In 2012-2013, authorities in Bayelsa State have relied on the services of the Italian surveillance company, Hacking Team, as evidenced in leaked emails from the firm.[170] During this period of 2012-2013, the state imposed a violent crackdown on online activists accused of spreading fear-mongering rumours. In 2014, the Citizen Lab, a group of Toronto's experts in cyber-forensics research, reported the presence in Nigeria of digital spying technology (known as FinFisher), which could gain access to individuals' computers or networks.[171]

The current framework supposed to regulate lawful interception of communications remains unclear in Nigeria, sorely lacking judicial safeguards against violations of citizens' privacy. Law enforcement agencies exert powerful influence over mobile service providers, potentially resulting in pervasive breaches of customers' privacy.[172]

### *Social Media Monitoring*

In recent years, governing authorities as well as political and business elites, have imposed tight control on spheres of information, with frequent intimidation and harassment against journalists, activists and bloggers that are considered critiques of the establishment.

## The Biometrics Assemblage

Biometric ID systems are making exponential advances across the African continent, with over 30 nations in the process of registering their populations' biometrics into centralized national databases.[173] Residents are increasingly required to use these new digital modes in order to participate in political and social life, such as voting in elections and accessing financial, health and education services. (Map 2 & 4)

Beginning of 2020, Kenya's biometric ID program was suspended by the High Court until the government enacts an appropriate and comprehensive regulatory framework that ensures personal data-protection and prevention of discrimination against minorities.[174] Judges on the High Court panel shared concerns with civil society organisations that the program was rushed into execution – biometrics data of about 40 million of Kenyans have allegedly be registered – but that specific ethnic subgroups were facing digital exclusion.

An analogue for the "Internet of Bodies and Minds," the term "biometrics assemblage" was coined by Madianou to describe the convergence of technologies that can learn to identify, measure and analyse populations' bodies and faces.[175] Along with demographic information, biometrics, including fingerprints, iris scan, facial scans, hand and lobe geometry – sometimes even voice and DNA samples – are captured either for one-time enrolment into an ID database or as continuing means of authentication. In this process, algorithms perform biometric data identification and verification, even if, when lacking optimal training datasets, they are prone to produce errors or amplify existing bias within biometrics measurements.

By making populations "legible" or "traceable," biometrics technologies are one method through which governments aim to secure borders, and are able to control which subpopulations are allowed to vote, benefit from health care, and participate in economic activities. As witnessed in Kenya, national biometrics ID systems are increasingly used by authorities to define who will be marginalized and who will benefit from public and private sector services.[176] Along the Somali border, in Garissa, a town that suffered recurrent violent attacks by the Shabab extremist group, a mother desperately tries to register her two daughters in Kenya's new biometric ID system, but she lacks the required birth certificates.[177] Born in Nairobi, a 73-old citizen, who served the government most of his life, has been refused the biometric

card repeatedly.[178] Authorities can impose additional security and ID requirements, making the registration process burdensome, or even out of reach, for minorities and vulnerable groups which end up being marginalised and unable to benefit from the digital economy's promises.

Increasingly, AI-driven technologies in the biometrics assemblage aim at capturing people's identity as they live, move and feel. For instance, facial recognition and biosensors (measuring gait, heartbeat, body temperature and sweat) detect individuals' faces and bodies in movement. Affect recognition is a technique within affective computing, a field that aims to interpret individuals' emotional states by teaching computer-vision algorithms to analyse their facial expressions and voice modulation, eye movements and pupil dilatation, gait and bodily reactions.

While affect-recognition lacks substantial scientific validity, the technique is already widely used in academia and industry to devise applications spanning medical pain management, retail advertisement, headhunting and student evaluation up to predictive policing and criminal justice. For example, police in the US and UK are using the eye-detection software Converus, which examines eye movements and changes in pupil size to flag potential deception.[180] Oxygen Forensics, which sells data-extraction tools to clients including the FBI, Interpol, London Metropolitan Police, and Hong Kong Customs, announced in July it also added facial-recognition, including emotion detection, to its software, which includes "analysis of videos and images captured by drones used to identify suspected terrorists."[181] In the streets of Johannesburg, the software iSentry, paired with facial recognition and webs of CCTV cameras, is programmed to detect and interpret "abnormal behaviour," pointing to the risk of automated forms of predictive policing.[182]

## Within Information Disorders: Automated Affective manipulation & Precision Biometric Attacks

The affect-recognition industry is growing exponentially and is thought to be valued over $25 billion.[183] Interest is growing to use affective computing – also called "emotion analysis" – in the political realm to test the potential appeal of ideologies and political candidates. After all, people also vote on emotions. For a neuro-marketing firm like Spark Neuro, success started with helping consumer brands and film companies achieve a high degree of "neuro-synchrony," when, across sub-populations, videos elicit strong emotions and electrify attention. Now, in a proof-of-concept, Spark Neuro recently began testing a sample of American voters, measuring neural (through electro-encephalogram) and physiological (sweat, heart-beat, pupil dilatation) data-points, to assess their responses to speeches of the 2020 Democrats' candidates.[184]

Several organisations have condemned not only the hype, but also the lack of rigorous scientific methods surrounding the current affect-recognition industry, and rightfully so.[185] The problem is that, even without scientific efficiency or backing, affect-recognition tools may become harmful if applied to the political and electoral domains. While these tools might not be efficient enough to shape elections towards a specific result, they might lead to increased disruption and polarization, electoral distrust and fatigue.

Again, what is highly problematic is the potential to misuse the convergence of affect recognition with pervasive data-capture technologies. Commodifying increasingly sensitive data about populations, affect recognition might serve the same PR and political consultancy firms that have been preying on citizens and vulnerable groups, like young voters in Kenya.

Emotional analysis already enables hyper-personalized campaigns in which key demographics are manipulated to affect voting behaviours at crucial times. Yet, as increasingly witnessed in cybercrime, the combination of psychometric tools and affective computing with personal datasets can help craft even more convincing emotion-targeting campaigns that can hardly be recognised as malicious.[186] Even the most experienced internet users might fall for such personalized attacks. Affective computing will also allow the deployment of political bots that can adopt human-like tactics to manipulate users. By promoting targeted propaganda, falsehood, confirmation biases, and incendiary content, AI-bots and algorithms may even play a growing role in information disorders. In the near-future, corporations in

the political influence business could rely on affective computing to identify the emotional triggers that push subgroups to violence, amplifying social engineering, psychological manipulation and other techniques of subversion and deception.

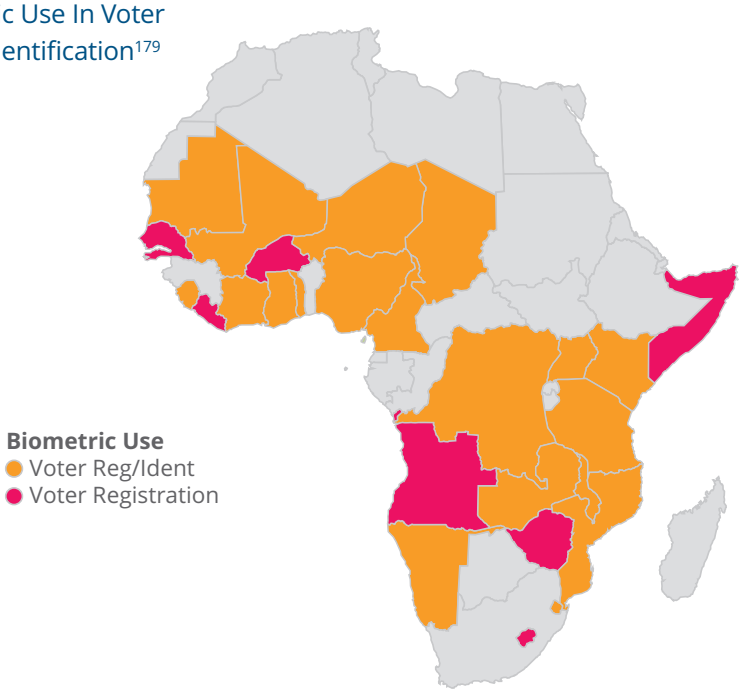
Large collections of biometric data about individuals confront them with another potential threat, what I call precision biometric attacks. In 2018, IBM detected an AI malware that can hide a cyber-threat, such as WannaCry, in a video conference application, and launch only when it identifies the face of the target.[187] According to the cybersecurity industry, the deployment of such biometric threats is not far on the horizon. Political candidates and influencers will also be targeted for impersonation through the synthesis and manipulation of video and audio samples, commonly labelled "Deepfakes."[188] Think of deep-learning algorithms able to design ever more sophisticated human impersonations based on biometrics analysis and behavioural mimicry.

With increasing ease, engineers can use deep learning generative models to automatically produce alternative, "synthetic" content such as images, video, text, and even realistic political speeches or news articles. In March 2019, cyber criminals used deep-learning voice spoofing to commit a cybercrime by reproducing the voice of a CEO, demanding a fake transfer of about $240,000.[189] The company Lyrebird developed a voice imitation algorithm that it says "can not only mimic the speech of a real person but shift its emotional cadence – and do all of this with just a tiny snippet of real-world audio."[190]

In August 2019, researchers in Israel published a new method for making Deepfakes by creating realistic face-swapped videos in real-time, with no extensive facial data-training. Deep-learning algorithms – called FSGAN – can pinpoint facial biometrics features in a video, then align the source face to the target's face.[191] Algorithms that do not need to be trained on each new face target provide a powerful toolkit to create realistic video forgeries at scale and with minimal know-how. In their article, the researchers warn about the potential for democratizing video forgeries: "Our method eliminates laborious, subject specific data collection and model training, making face-swapping and re-enactment accessible to non-experts."[192]

It is crucial to analyse and understand how countries in Africa might perceive a threat by synthetic media in a different light than states in the West. South Africa was at the core of an interesting research project on Deepfakes led by the Witness group, a research lab focused on digital media.[193] Participants from South Africa expressed significant concerns over the use of Deepfakes by ruling political parties to incite violence beyond generating disinformation. Their concerns were heightened by the potential for Deepfakes to spark mob violence in areas suffering

**Map 4** | Status for Biometric Use In Voter Registration and Identification[179]



> Increasingly, AI-driven technologies in the biometrics assemblage aim at capturing people's identity as they live, move and feel.

from political or ethnic tensions. Similar digital manipulation already happened in South Africa when manipulated videos were spread in the context of xenophobic attacks targeting Nigerian businesses.

In a nutshell, biometric ID systems give state, technology vendors and private sector actors access to citizens' sensitive information – their "digital bodies and minds" – which can become the object of additional forms of affective manipulation and new types of precision biometrics attacks. According to the U.N. High Commissioner for Human Rights, biometric data "is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights."[194] Adequate safeguards are often not in place to protect populations from harmful implications related to privacy and data security.

## As Emerging Web of Surveillance: Smart and Safe Cities

Combined with facial-recognition and close-circuit TV cameras, biometric ID systems are also one prevailing way to impose new forms of bio-power on populations, seriously influencing privacy and self-determination. According to the U.N. High Commissioner for Human Rights, "biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. [...] Against that background, it is worrisome that some States are embarking on vast biometric data-based projects without having adequate legal and procedural safeguards in place."[195]

The technologies converging in the biometrics assemblage have made it possible to computerize surveillance, policing and intelligence collection. Following China's model, several governments, including in Kenya, South-Africa, Nigeria and Zimbabwe, are considering multi-million plans to erect "Smart and Safe cities,"[196] which are essentially centralized architecture for social and behavioural control. These modern cities rely on an integrated platform, which collects multi-layers of data streams: 1) from facial-recognition devices often connected with CCTV cameras, and 2) from WIFI and phone scanners, devices that can monitor, sometimes even intercept, mobile phone or wireless network activities and communications. Such platforms also aggregate data from financial, health and criminal records, as well as national ID cards and licence plates captured at checkpoints. Most smart and safe cities ultimately aim to integrate biometrics from voter registration and digital identity systems. Through this matrix of interconnected data streams, algorithmic programs can track populations, searching for patterns of unusual behaviours.

In 2018, as a recipient of China's Belt and Road technological development program, the government of Zimbabwe signed a series of contracts to deploy networks of CCTV cameras connected with facial-recognition software across cities' infrastructure, from public transport (bus stations, railway and airports) and linked to data from health and smart financial systems.[197] The Chinese company, CloudWalk, will use its 3D light facial software, which is more accurate at detecting the facial features of dark-skinned populations, to build a database of Zimbabwean citizens, comprising their faces likely matched with other biometrics.[198] Such a national identity system paired with compulsory SIM card registration data creates the architecture for precision population surveillance, from physical movements to online activities. Essentially, it builds networks of digital bodies and minds that can be harnessed within Zimbabwe' securitization agenda.[199]

For China, the technological and economic advantage is significant and multifaceted as it comes with a comprehensive suite of corporate collaborations

> Affect-recognition tools may become harmful if applied to the political and electoral domains.

in data-infrastructure and biotechnology: getting access to new substantial data-markets, including individuals' consumption, behavioural, biometric and biological data; gaining know-how into training algorithms on darker-complexioned populations; perfecting the surveillance function of converging technologies. In addition, it increases Zimbabwe's dependency on China's economic and security industrial complex; and finally, creates more opportunities for natural resource-capture, from genetics to rare earth minerals.

## In South Africa

South Africa presents a scenic and powerful example of the biometric assemblage. For more than a decade, the surveillance industry has grown webs of CCTV cameras equipped with analytic software to prevent crime and enforce local security. The story started with promises to deploy fiber-optic internet networks to households, building the infrastructure that would later allow high-tech surveillance to thrive in Cape Town and Johannesburg, progressively expanding to suburban neighbourhoods. In 2019, Vumacam, the surveillance company at the core of this CCTV revolution has covered most of Johannesburg' suburbs and has its eyes on equipping Johannesburg with 15,000 cameras.[200]

Coupled with AI, facial-recognition and sensing technologies, today's CCTV networks are like "sharp eyes," that use algorithms to scrutinize populations' movements for "abnormal behaviours." They can track objects, license plates, clothing colours, human quirks and faces. Vumacam' surveillance apparatus incorporates an assemblage of cutting-edge technologies: iSentry is a software made by the Australian military to detect "unusual behaviour;" BriefCam is an Israeli software program made to summarize human actions in a video for forensics investigation; the two software programmes are connected to a centralized repository of video data that can be shared with security providers, government agencies and other third parties. With facial-recognition devices and mobile fingerprint machines, the biometric assemblage can be used for corporate and commercial surveillance, as well as for profiling and predictive policing. In Johannesburg, Vumacam is also in the process of extending its CCTV networks to public schools under the "Kids Custodian Initiative."[201]

> "Commodifying increasingly sensitive data about populations, affect recognition might serve the same PR and political consultancy firms that have been preying on citizens and vulnerable groups, like young voters in Kenya.

> "The technologies converging in the biometrics assemblage have made it possible to computerize surveillance, policing and intelligence collection.

With this South African version of the Internet of bodies, the public lives of communities are being watched by a privatized surveillance infrastructure. Yet, these networks of "sharp eyes" high-resolution cameras powered by algorithms, embody pervasive biases produced by decades of data about what constitutes "abnormal behaviour" in a residential area of Johannesburg. Scholar, Michael Kwet, from Yale Law School, argues, through its decade-long investigation of South Africa's surveillance technologies, that defining "abnormal behaviours" may lead to problematic and biased practices of predictive policing.[202] From skin tone, scars, gait and clothing, populations in South Africa – one of the world's most racially and economically divided countries – face a new surveillance era with corrosive ramifications for social justice and electoral stability.

## The Global Supply Chains of Surveillance

A complex amalgam of foreign corporations has played an instrumental role in helping generate and spread information disorders in multiple elections across Africa, in Kenya, Nigeria and South Africa. Some corporations provided data-analytics and P.R. or "reputation-laundering" campaigns that turned

into powerful tools for invading spheres of information and influencing the behaviour of voters. Some would broker deals across the world to sell the latest surveillance technologies, providing in a comprehensive package the tacit knowledge of cyber-mercenaries. The former represents an aggressive form of surveillance capitalism and, the later, the rise of a new transient security industry. Both are multi-million influence businesses that are part of a larger ecosystem that this report calls the "global supply chains of surveillance."

**The Political Influence Business:** The SCL Group, Cambridge Analytica, Harris Media and Bell Pottinger are the most sinister examples of a much bigger industry centralized around harvesting, analysing and weaponizing population data to shape electoral and political campaigning. Yet, this powerful and opaque corporate system, which thrives on our personal information, involves hundreds of companies and subcontractors that operate in developed and developing markets. They include private data-brokers (such as in the health and insurance sectors), data-analytics firms (*HaystaqDNA* specialises in U.S. voters' profiling), political consultancies (*270 strategies* crafts strategies to mobilize segments of the electorate), and marketing companies (*eXelate* uses data to create personalised ad campaigns to target phone users).

We have exposed in section III the harmful, destructive implications produced by the SCL Group, Cambridge Analytica, Harris Media and Bell Pottinger during electoral campaigns in Kenya, Nigeria and South Africa. But, for decades, companies in the strategic influence business – like the SCL group – have run much larger data-mining operations without oversight, under a "surveillance-first," "accountability-later" governance model.

In 2014, Ghana's Health Ministry commissioned the SCL Group to run a survey on health practices and needs involving 30,000 households in 97 constituencies across 10 regions.[203] The next move of SCL was to propose its services to the then ruling National Democratic Congress (NDC) party, offering to "model the future vote distribution within each constituency in Ghana based on how respondents said they would vote should there be an election tomorrow." Using funds from Ghana's Health Ministry, the SCL group was in a position to sell demographic data coupled with "a large scale dataset related to various aspects of public health in Ghana" and "data on themes including which national and local issues are important to people, their perceptions of the state of the economy, popular media channels, and key influencers." In the years 2009-2012, the SCL group was also contracted by UNICEF to develop a communication campaign on preventing child marriage and in 2011 by UNDP to study disarmament in South Sudan.

Most of SCL's data-mining operations, supported by domestic actors and international donors, sorely lacked adequate measures for protecting populations' privacy and data-security.

**The Biometrics and AI Surveillance Industry:** The global biometrics market is exploding, expected to top $50 billion by 2024.[204] Yet, the global supply chains of biometrics and AI surveillance are complex, fragmented and relatively heterogeneous, involving private technology and services from several tech-leading nations. According to Global Market Insights, North America, with U.S. Palantir, Cisco and IBM at the forefront, will represent more than 30% of the overall biometrics industry share by 2024. European leaders in the field, such as the French company Gemalto and the German company DermaLog play an active role in the deployment of new biometric ID projects across Africa (Map 2 & 4). U.S. and European providers are in competition with China's Laxton Group, which has deployed nation-wide biometrics and digital ID systems for elections in Malawi, Mozambique, Tanzania, Colombia, Indonesia, Saudi Arabia, Guinea-Bissau, and South Africa.

The business of building biometric voters databases is an extremely lucrative one: for instance, the initial contract signed by the French contractor, Idemia, with Kenya's government for the new biometrics ID system was close to $74 million.[205] The German firm, DermaLog, offered its services to Nigeria for about $50 million;[206] and China's Laxton Group offered its biometric services to Zimbabwe for about $4 million.[207]

Live facial-recognition and algorithmic surveillance has also become a highly lucrative business particularly for China, which provides such technology in more than 60 countries with about half of them participating in loan programs under China's Belt and Road Initiative (BRI).[208] [Map 5]


© Unsplash/Pretoria

BRI's economic support often comes with mandatory clauses for recipients to contract with Chinese technology providers. A large corporate group like Huawei is aggressively deploying AI surveillance ventures in the Sub-Saharan region, bringing technologies and expertise to about 50 countries.[210] Huawei's effort includes wide development of CCTV cameras equipped with facial-recognition and data-optimization capabilities, such as in Nairobi's $172 million Smart and Safe City project, Uganda's $126 million urban surveillance system, and a similar long-term venture in Mauritius (called "Inspiration for Heaven"). In Uganda and Zambia, Huawei experts have allegedly shared techniques to track the movements and communications of political activists.[211] Uganda's smart surveillance system might be partially deployed before the coming elections. The developer, Hiksvision, which has installed surveillance technologies in Xinjiang, has chosen South Africa as a base of operations for the continent, and is also involved in Zimbabwe where it collaborates with CloudWalk on smart policing.[212] In April 2019, the Chinese company Transsion became the dominant player in Africa's mobile market, overtaking Samsung, and unveiling a new affordable phone with integrated facial-recognition software.[213]

While a substantial hype surrounds smart and safe city projects run by Chinese firms in Sub-Saharan Africa, it is worth looking at the map below showing the reach of Sino-technological ventures, capturing "digital silk roads" for fiber-optic and 5G networks, cloud-computing and data centres. (Map 5)

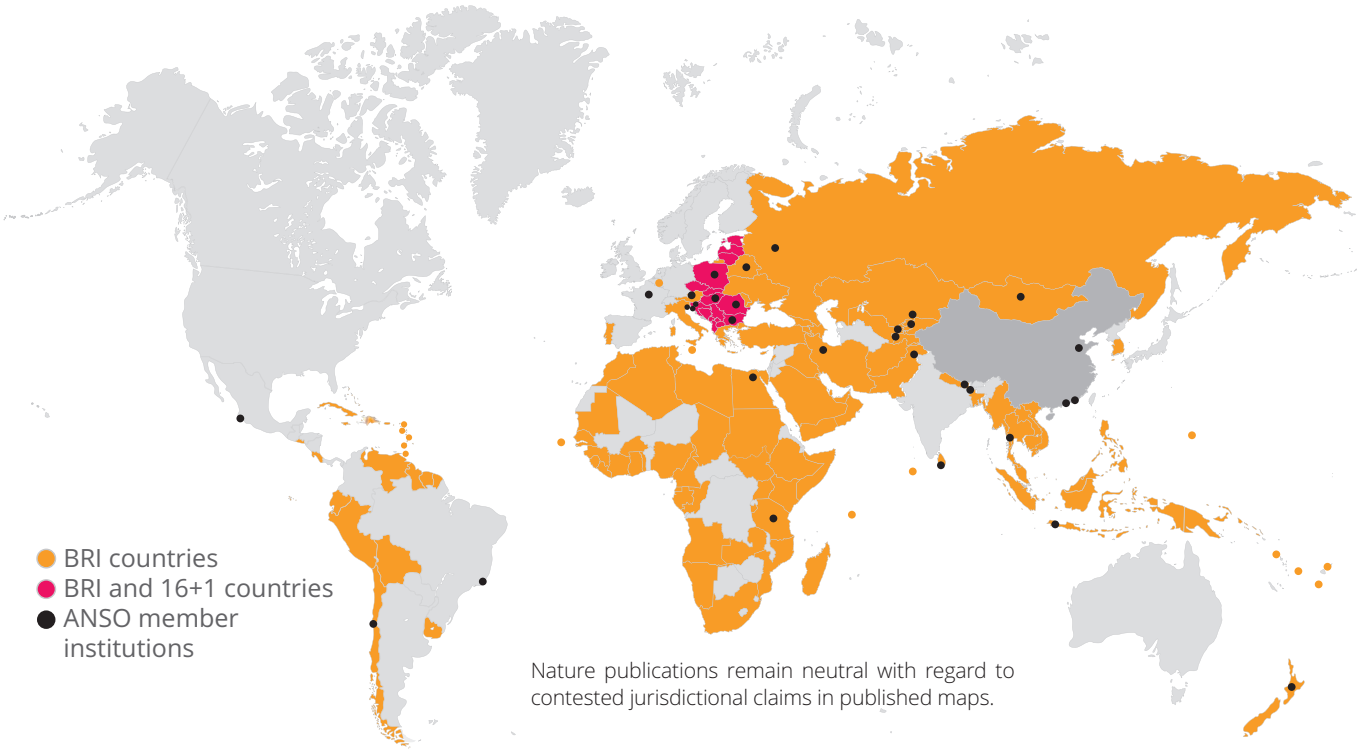
After China, the next supplier of AI surveillance is Japan's NEC Corporation exporting its technology to about fourteen countries, mainly in the Global South, and has partnered with the UN over a development project across the African continent.

In addition to biometrics and AI technologies, the private cyber-surveillance industry presents another domain to watch. It is also made up of complex supply chains, a mercenary-like, secretive industry, involving defence and intelligence contractors, software companies, hardware vendors, and even traditional telecoms. In a report to the UN Human Rights Council, the UN Rapporteur on the promotion and protection of the right to freedom of opinion and expression warned about the pervasive lack of oversight in an industry which presents serious potential for technological proliferation.[214]

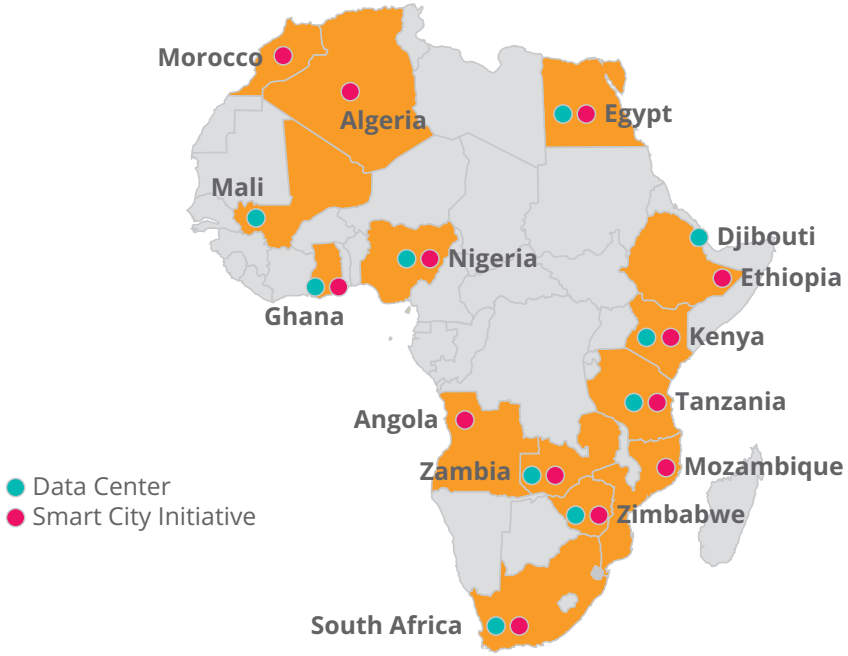
> “For decades, companies in the strategic influence business – like the SCL group – have run much larger data-mining operations without oversight, under a “surveillance-first,” “accountability-later” governance model.

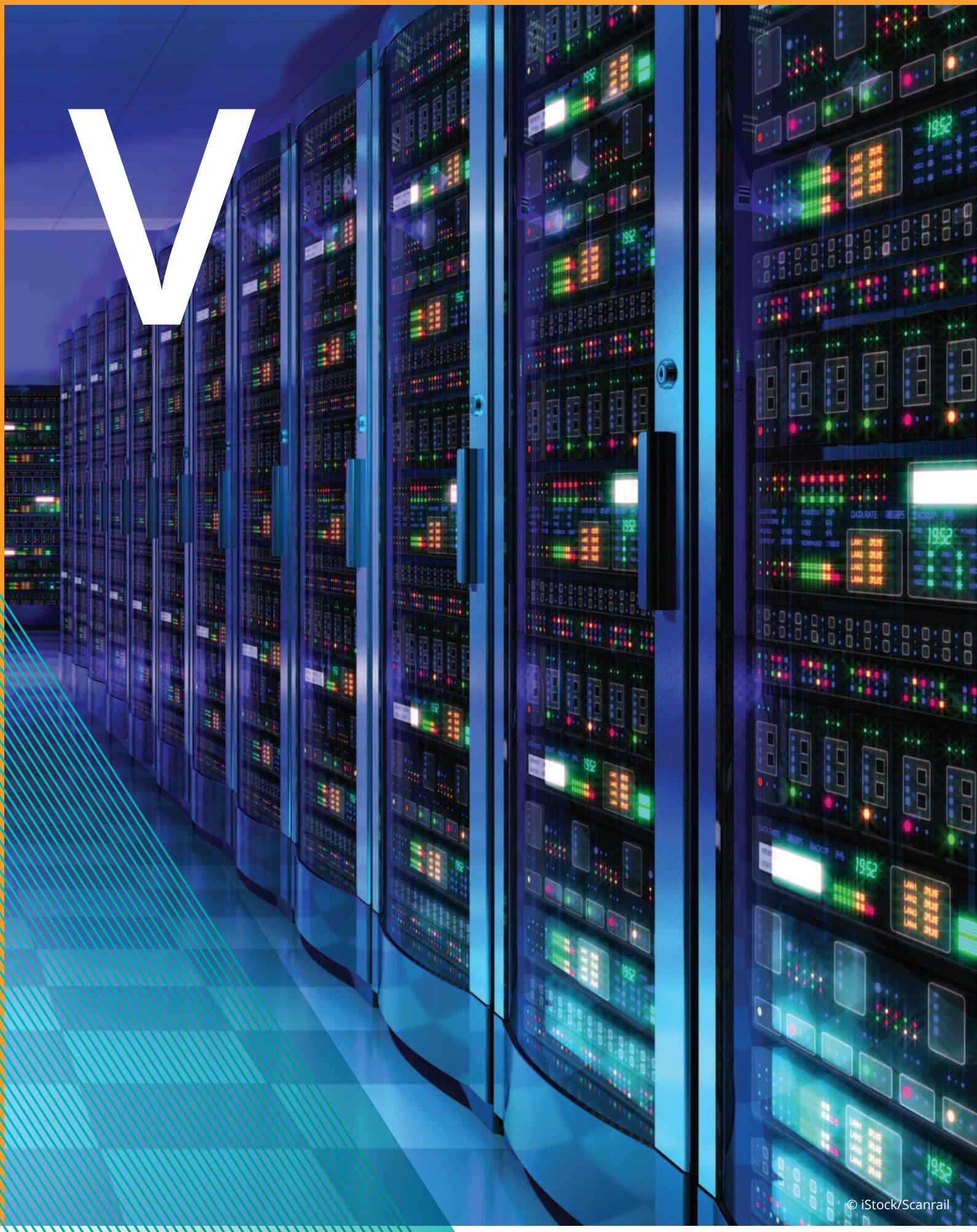
**Map 5** | China's Belt & Road Initiative, 2019[209]

**Growing Network**
The Belt and Road Initiative (BRI) operates at many scales. More than 120 nations have signed agreements with China and 37 academic institutions have joined the Alliance of International Science Organizations in the Belt and Road Region (ANSO). Sixteen nations have joined with China to form the 16+1 organization, formally known as the Cooperation between China and Central and Eastern European Countries.




**Map 6** | China's Data Centres & Smart Cities, 2019[215]





# CYBER-SOVEREIGNTY, MULTIPOLAR COMPETITION AND THE RISE OF CONVERGING RISKS FOR AFRICAN POPULATIONS

Every cell phone, a living brain. This is how emotion wars were manufactured and spread.

Across Africa, at election times, there are pervasive cognitive-emotional conflicts being waged for the control of populations' thoughts, emotions and attitudes. These "emotion wars" exacerbate societal and ethnic tensions and amplify public polarization. They increasingly condition and limit notions of self-determination, and could continue to do so with future generations to come.

In the last decade, the predatory practices of corporations in the political consulting and strategic intelligence business have been exposed, coming to light as growing existential threats to democratic processes, in particular elections. Cambridge Analytica, the SCL group, Bell Pottinger and others, made millions out of commodifying, without consent, large amounts of population data to manipulate political attitudes and engineer behavioural reactions, inflaming tensions and violence. Yet, it is worth noting these corporations are part of larger, tentacular global supply chains of surveillance thriving on a private industry composed of cyber-security, military and intelligence contractors, often operating in mercenary style.

## State Power and Securitization Agenda

There are more challenges and threats to election security than data-predation by the global private surveillance industry. When analysing the anatomy of information disorders in Kenya, Nigeria and South Africa, we also have to consider their role in domestic politics. How are information disorders engineered for strengthening state-power? For state actors, information disorders are essentially a battle waged through the instrumentalization of population data and modern digital technologies, to impose real-world dynamics of power and resource capture. Controlling populations' "digital bodies and minds" is the ultimate, post-modern form of biopolitics. It can be used for winning elections and preserving, even securing state-power.

**Tensions around the Digital Economy's Social Contract:** What is the balance between individual rights and state-command of collective security and prosperity in the digital economy? Policymakers across the world face this question, but in several African countries where large-scale population data-optimization projects have started in a context of limited accountability, the question is being posed with urgency.

New forms of digital authoritarianism increasingly compete with liberal democracies over how to most effectively exploit and control technological governance models to ensure that AI and data-capture technologies contribute to social order with a minimum of distributed progress and benefits.[216]

When devising regulatory instruments for the converging tech economy, governments in Kenya, Nigeria and South Africa face this tension between a digital surveillance model and a more open, liberal model that might also reduce state actors' power and control over populations and resources. The free-market, liberal option might come at a high price for national governments that are struggling with instability and do not yet have the competitive advantage of a global tech-leader like the U.S.

> "Across Africa, at election times, there are pervasive cognitive-emotional conflicts being waged for the control of populations' thoughts, emotions and attitudes.

Despite pervasive infringements on human rights and limits to individual agency, China could emerge as a model of digital economy that has embraced the support that AI and surveillance technologies provide to governance. The commodification of massive streams of populations' data means that, in the future, governments may be able to not only monitor and control the behaviours of individuals, groups, professions and media communities, but also produce financial value to be further invested in the digital economy. In brief, digital authoritarian regimes could ensure state-preservation – with its dynamics of resource capture – and provide security under the form of a repressive social order.

Governments in Africa may increasingly see the dark side of the digital economy: its potential to threaten regime stability. In the context of heightened insecurity and proliferation of cybercrime, many countries struggle to secure their own cyber infrastructure. China's cyber-sovereignty model may therefore provide an illusion of proactive, tactical methods to manage external threats, mitigate cybercrime, and control disinformation campaigns, while offering new means to censor public opinion and prevent large-scale demonstrations.

> "Controlling populations' "digital bodies and minds" is the ultimate, post-modern form of biopolitics. It can be used for winning elections and preserving, even securing state-power.

**Cybercrime Laws and "Disinformation Laws:"**

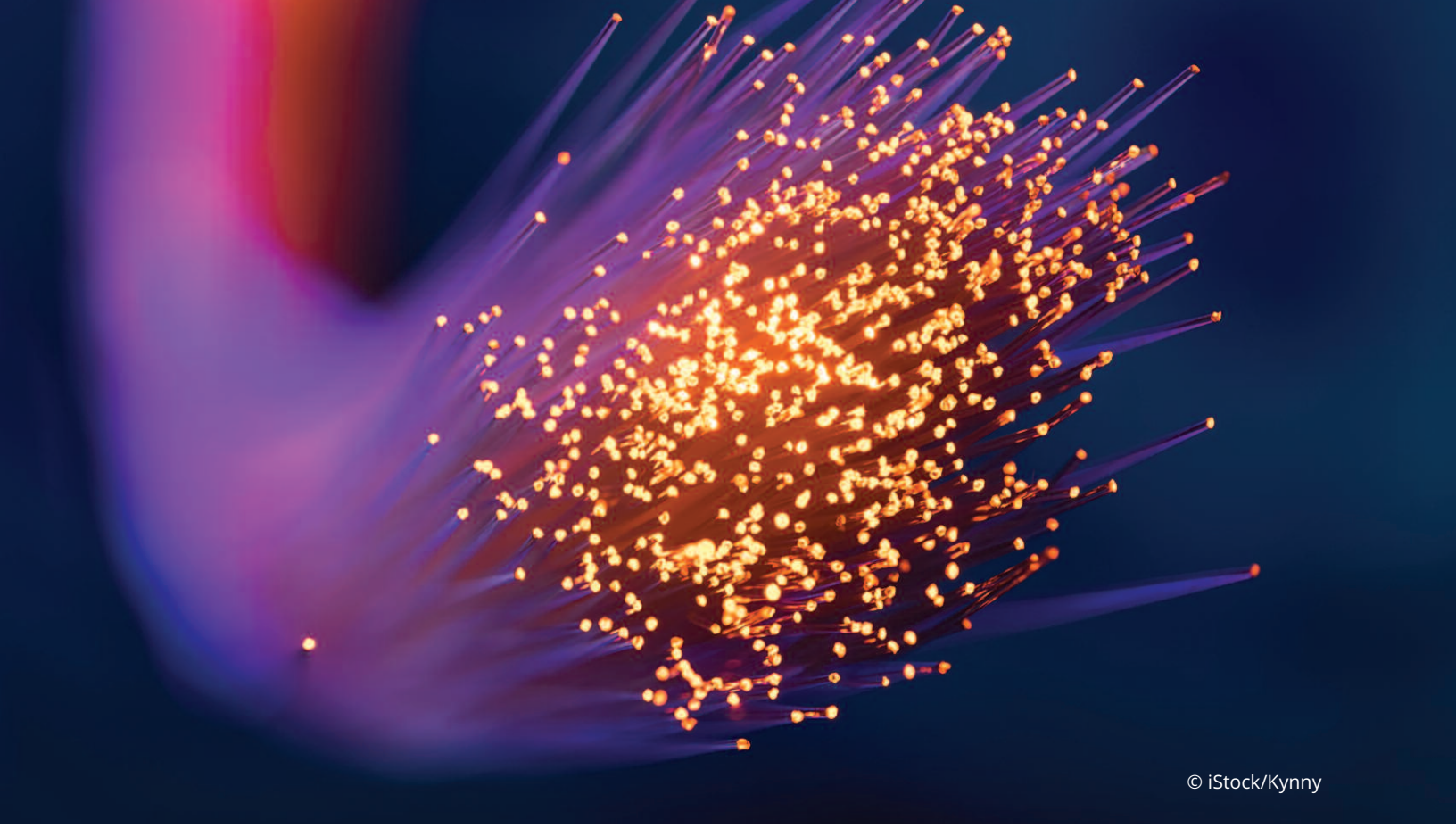
For several states in Africa facing rising domestic pressure the ability to control spheres of information is part of a "survival strategy" to preserve regime stability. These governments have direct interest in overseeing and censoring content and information that could undermine, even imperil, domestic stability and regime legitimacy. In recent years, a series of cybersecurity legislation have been proposed and passed by states in Africa in the name of defending and protecting national interests, even if at times such legislation violates individual rights. In many cases, the ultimate goal in those attempts to govern cyberspace had been regime-preservation. Beyond the direct violations of human rights and freedom of expression, the risk for populations is the closing of "virtual civic space."

**In Kenya:** Civil society organisations have criticized an alarming trend of laws on hate speech and defamation being frequently instrumentalized to silence opposition to Kenya's government.

The Computer Misuse and Cybercrimes Act, 2018, which was passed by the government in May 2018, is a powerful tool for the Kenyan government to prosecute online critics of the regime. The Cybercrime Act imposes charges of up to 10 years in prison for the publication of "false" or "fictitious" information that leads to "panic" or is "likely to discredit the reputation of a person."[217] In May 2018, the Bloggers Association of Kenya (BAKE) made the argument that substantial provisions in the Cybercrime Act could give the government extensive discretion in monitoring personal communications and prosecuting individuals acting in the public interest, such as government whistle-blowers. BAKE successfully appealed 26 sections of the law, which are still suspended.[218]

In 2017, Section 132 of the Penal Code was ruled unconstitutional by the High Court in Nairobi. Authorities had increasingly relied on Section 132 to penalize both online and offline speech that was deemed "undermining the authority of public officers."[219] Civil society activists made the successful argument to the Hight Court that the provisions were vague, uncertain and an unjustifiable limitation to freedom of expression, as well as violating basic criminal law principles.

Hate speech is also penalized under the 2008 National Cohesion and Integration Act, which was approved in the wake of the dramatic ethnic violence during the post-2007 election period. Individuals found guilty of spreading hate speech, broadly defined, can be fined up to 1 million shillings ($11,000), sentenced to up to three years in prison, or both. During the 2017 elections, charges for alleged hate speech were used against social media users, including blogger Paul Odhiambo, who was arrested for spreading alleged hate speech on Facebook and WhatsApp.[220]



© iStock/Kynny

**In Nigeria:** In March 2019, President Buhari declined to sign the Digital Rights and Freedom Bill, which would have provided the required legal framework to better protect human rights online. The bill has been revised to address the concerns expressed in March 2019 by President Buhari that the bill "covers too many technical subjects and fails to address any of them extensively."[221] The bill was reintroduced in the House in July 2019.[222]

In 2015, Nigeria's government passed the Cybercrime Act, aiming to drastically reduce the expansion of cybercrime.[223] Yet, the law distinctly lacks a clear definition of what cybercrime is and how digital technologies can be misused for criminal purposes. Such strategic omission creates legal uncertainty that has already been exploited to bypass human rights' protection and criminalize the online behaviours of civil society, media, and other public critics of the regime. Numerous social media influencers, online journalists, and private citizens were charged for "cyberstalking" under the Cybercrime Act, even in the absence of convictions.[224]

In March 2018, the Senate also proposed a draft hate speech bill, which would prescribe the death penalty for speech that leads to an individual's death. The draft bill led to strong opposition and has not been approved yet by the Senate.

## Multipolar Competition

Beyond domestic governance, information disorders also have geostrategic and geo-political ramifications. They are symptomatic of a wider multipolar competition for normative influence in cyberspace. The rise of complex tech-driven surveillance regimes exploited by states to control populations reveals the changing power dynamics of cyberspace. Slowly, on the global scene and in absence of a global digital governance framework, the prevailing geostrategic model might become cyber-sovereignty or cyber-nationalism, a model that centres around digital surveillance and control without oversight by and accountability to a multinational body.

> "Beyond domestic governance, information disorders also have geostrategic and geo-political ramifications.

In a context of multipolar competition, ruling elites in states such as Kenya, Nigeria and South Africa have to decide what cyber-governance model will help them safeguard their sovereignty, while at the same time not becoming dependent on external actors economically or for their cybersecurity needs. The governance options they will take are heavily influenced by the tech-leading nation they partner with.

**Tensions around the Digital Economy's Global Supply Chains:** Governments in African countries face a set of questions that pertain to competition and control over the global information infrastructure and supply chains of the digital economy. What level of control over information infrastructure and converging tech supply chains is needed to compete and secure a future in the digital economy? What kind of relationship should exist with private sector actors – in the national digital ecosystem, but also inevitably in the global supply chains of converging technologies? Can the private sector ecosystem be tightly controlled by the state? Is it possible to build-up a home-grown sector, or will it largely depend on capacity-building by other more advanced technological nations? How will the reliance on tech-leading nations potentially shape or even limit state-power?

While countries like Kenya, South Africa and Nigeria are already deploying with success transformative digital economy' services, they still face sustained financial and capacity building challenges, and as importantly, they lack a robust legal framework to safeguard civil and political rights and ensure meaningful accountability. They are therefore likely to partner with tech-leading nations to build the required information infrastructure and import the converging technologies' expertise needed to secure integration into the global digital economy. The countries they chose to partner with will inevitably bring and potentially impose specific technical standards, proprietary agreements, and equally might influence the norms of governance.

At the same time, on the global scene, Kenya, Nigeria and South Africa represent an Eldorado of growing digital markets with access and control over large populations' data, as well as energy, biodiversity and mineral resources needed to power the digital economy. Even more, they constitute different geostrategic territorial corridors where to build future 5G digital architectures made of cloud-computing and satellite data centres as well as extensive networks of fiber-optic cables.[225] At the centre of a rising multipolar competition, governments in Kenya, Nigeria and South Africa will determine which governance model will help them secure relative economic growth and autonomy without endangering regime stability.

In the competition over who will gain geostrategic positioning in African countries, Silicon Valley platforms and U.S. military contractors provide high technology and know-how, but very limited regulatory instruments in exchange to their prospect of commodifying new data-markets. Silicon Valley's model of regulatory-free innovation offers limited answers to managing privacy and accountability gaps.

With their proposed regulatory model promoting responsible innovation and social justice, nations in the EU could constitute a normative role-model for African nations. Beyond powerful normative aspirations though, the EU's engagement is thin when it comes to concrete regulatory leadership, technological export and capacity-building. Moreover, it is unclear if the high-level data-protection standards enacted in the EU's General Data Protection Regulation (GDPR) could be effectively translated into operational and accountability mechanisms when private sector actors partner on data-mining projects with African countries. European companies have already lent their tools and expertise in biometric voting technologies to several African countries, including Kenya and Nigeria, with no clear, operational playbook on how to preserve individuals' consent and privacy.[226]

> "On the global scene, Kenya, Nigeria and South Africa represent an Eldorado of growing digital markets with access and control over large populations' data, as well as energy, biodiversity and mineral resources needed to power the digital economy.

China does not provide African nations with regulatory guidance or guarantees in terms of privacy and meaningful public accountability. But, along with its massive economic backing, China proposes to export another normative model centred around pervasive state control of populations and their information infrastructure.[227] Such form of cyber-biopower normalizes political and social control over citizens as well as a securitization agenda based on digital surveillance. It essentially merges the imperatives of national security with those of regime stability. The promise is to provide populations with both, economic growth and collective security, under a repressive social order and with limited political agency by citizens themselves. While this type of digital authoritarianism could still spur public backlash for ruling political elites, it nevertheless allows them to strengthen their power.

In exchange for financial and technological support, China seeks both systematic long-term engagement to legitimize its normative influence, and strategic positioning to build and control the digital roads of cyberspace.[228]

> China seeks both systematic long-term engagement to legitimize its normative influence, and strategic positioning to build and control the digital roads of cyberspace.

## The Sino-African Roads to Converging Tech Futures

For decades, China has nurtured close relationships with the political elites of several African growing economies, in particular those that have strategic mineral and biological resources.[229]

But, starting in 2013, ad-hoc collaborations gradually turned into an ever-expanding network of Sino-African science and technology agreements under President Xi Jinping's ambitious infrastructure-development program, the Belt and Road Initiative (BRI). That program whose sizeable investment is estimated at $1 trillion supports China's collaboration with more than 130 nations through motorways, high-speed railways and marine ports to increase China's global reach into the digital economy.[230] Among those nations, 40 out of 55 African countries and the African Union Commission signed BRI scientific development agreements, from AI and satellite imagery projects to genomics agriculture.[231] China has become the largest investor in African critical digital infrastructure and a partner of choice for research development and education with thousands of scholarships offered each year to African PhD students.

Across Africa, particularly in coastal countries, China's long-game is to control enough territorial, maritime and economic corridors to become concurrently the first technological provider to oversee inland critical digital infrastructures (AI data centres, observatory satellites, cloud environments, e-commerce platforms, and smart cities), as well as the web of fiber-optic cables built along railways or undersea, that will power 5G networks and a substantial part of the global Internet grid.

Some experts have, with reason, criticised BRI's grand plan for lacking a long-term funding strategy with substantial foreign direct investment. Recipient countries have expressed concerns over debt sustainability, environmental impacts and overall economic viability.

But what the "Maritime, Economic and Information Silk Roads" unveil is the importance of Africa as a geostrategic positioning to provide access and control over growing transnational and critical information infrastructure and data-reservoirs that will power converging technologies, from AI, cloud-computing, to genomics. This technological upheaval is already shaping the future of global digital services, from high-tech finance to precision medicine. In November 2018, WeChat, the financial and social media platform, launched a partnership with M-Pesa, Kenya's ubiquitous payment platform, the two companies' combined networks playing a substantial role in the trade flow between China and East Africa.[232]

In addition, China has secured access to much of the world' supply of strategic metals and minerals crucial for deploying new technology, and substantial amounts of those come from Africa, including lithium, rare earth, copper and manganese used in

everything from smart phones to electric cars. China also owns WuXiNextCODE, the largest global genomic data platform using machine-learning to better diagnose rare diseases and cancer as well as to design tailored, improved therapeutics.[233] Controlling the behavioural and biological data that will fuel AI and genomics research translates into significant economic and security assets. Whoever gains a monopoly of these powerful resources may well be able to influence the well-being of entire populations and impact innovation in allied countries.

With the digital revolution too, competitive advantage comes not only with territorial access but also the African governments' willingness to share – sometimes *de facto* lend – the resources required for digital supremacy. Another form of strategic lock-in comes from being the first to decide which proprietary equipment and technical standards will characterise cloud data centres and 5G networks. The ultimate goal is to gain extraterritorial control over transnational critical information and technological infrastructure. A telecom giant like Huawei – in partnerships with a few other Chinese companies – could therefore control which data-driven services (from virtual reality, telemedicine, genomics research, and e-finance) will reach and use China's 5G networks and cloud platforms.

> Controlling the behavioural and biological data that will fuel AI and genomics research translates into significant economic and security assets.

**5G Digital Roads:** Chinese telecom equipment makers – including Huawei and ZTE – will likely continue to play a prevailing role in deploying 5G networks across BRI African countries, imposing related technical standards, and leveraging connections with Chinese authorities to win access.[234] Huawei is in charge of building the PEACE cable, a fiber network that connects Asia to Africa, and then reaches towards Europe at speeds of 16 terabytes per second. The Chinese telecom giant has already completed a 3,750-mile cable between Brazil and Cameroon.[235] With government support, Huawei can deliver high-quality fiber-optic cables at lower costs

> Strategic lock-in comes from being the first to decide which proprietary equipment and technical standards will characterise cloud data centres and 5G networks. The ultimate goal is to gain extraterritorial control over transnational critical information and technological infrastructure.

than European and U.S. competitors. The telecom giant has already built substantial parts of Africa's 4G networks (and most of the 2G and 3G) and has become in form of the company Transsion, the largest low-cost mobile phone provider in Africa.

In September 2018, the Exim Bank of China loaned $328 million to the Nigerian government to build a Huawei-commissioned telecoms network.[236] By early 2020, Huawei held 28% of South Africa's mobile phone market and is also partnering with digital services' provider Rain to build 5G networks.[237] Kenya's biggest telecom operator, Safaricom, is in the process of contracting with Huawei to deploy 5G networks.[238]

**Cloud Data Centres:** The rise of cloud computing in Africa is also leading to soaring demand for data-optimization capacity localized on the continent. Coastal countries will emerge as investments hotspots for building data centres that will have direct access to subsea cables allowing for greater regional connectivity. China has already exported data infrastructure capacity in Asia, opening data hubs in Hong-Kong in December 2017, Singapore in March 2019, and Japan[239] and Indonesia in January 2019. Yet, North-Africa increasingly presents other strategic coastal opportunities. In February 2019, Huawei launched its first data centre in Egypt, which conveniently borders the corridor that connects East Africa to Europe. The Chinese telecom also signed a contract with the Algerian government to build a data centre for its custom and border authority. With BRI agreements signed with Morocco, Algeria, Tunisia and Egypt, China has a footprint in the Mediterranean.[240]

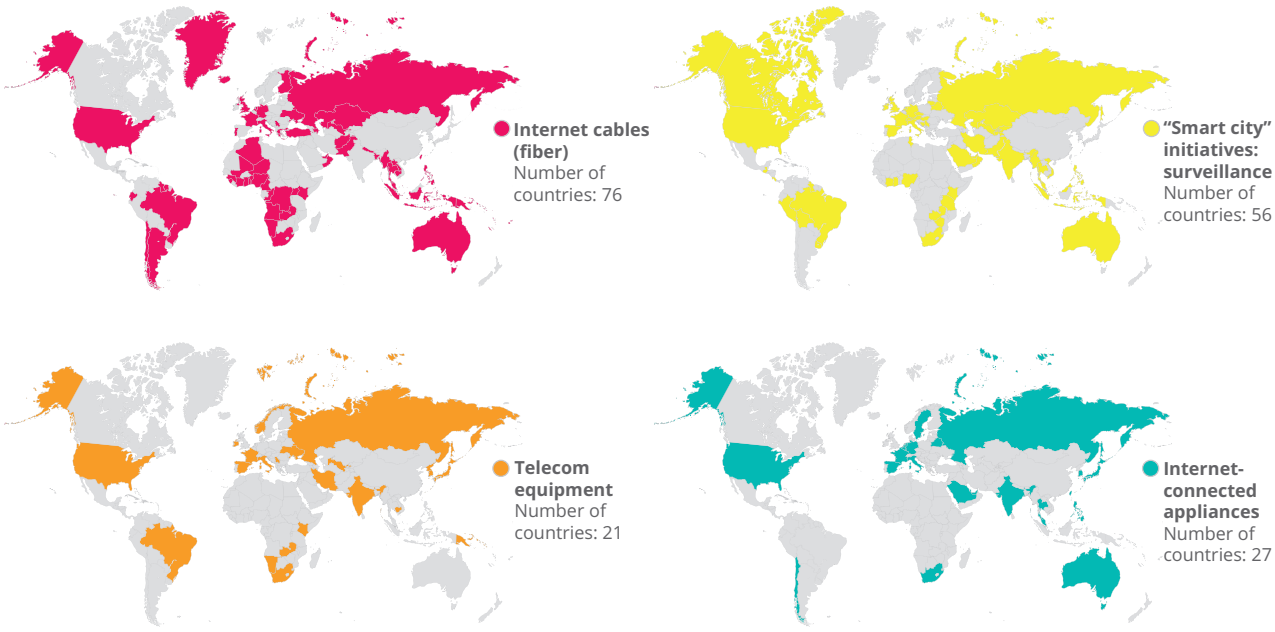
The U.S. and Western allies also own thriving AI and advanced computing platforms that have recently invested in African nations, but in a more fragmented, less systematic fashion. In South Africa, Boston-based private equity firm Berkshire Partners is backing Teraco Data Environments, which is one of the largest and most interconnected data centre hubs on the continent. In 2019, Microsoft has also launched data centres in South Africa which already accounts for half of the continent's data centre capacity. In the coming months, Amazon will open a cluster of data hubs in Cape Town. London-based private equity firm, Actis, is injecting $250 million into cloud computing capacity, starting with Rack Centre, a leading Nigerian company that serves the west African market.[241]

In a nutshell, today's multipolar competition between China's tech giants and large private internet platforms from the West is about controlling cyberspace transnational information infrastructure and its data-flows; gaining access to strategic intelligence about Africa's soft capital future (growing digital markets, revealing the needs of populations that might be doubling by 2050); overseeing converging technologies global supply chains; and gaining competitive advantage in global value chains.

Semi-authoritarian regimes in Africa, a significant number of which are involved in the BRI, are increasingly interested in China's use of the internet to control populations' digital bodies and minds. It provides opportunities to shape the governance of national cyber-domains in ways that normalize a securitization agenda with potential for surveillance, censorship, and repression of political opponents.

> "The rise of cloud computing in Africa is also leading to soaring demand for data-optimization capacity localized on the continent.

**Map 7** | China's Footprint, 2019[242]

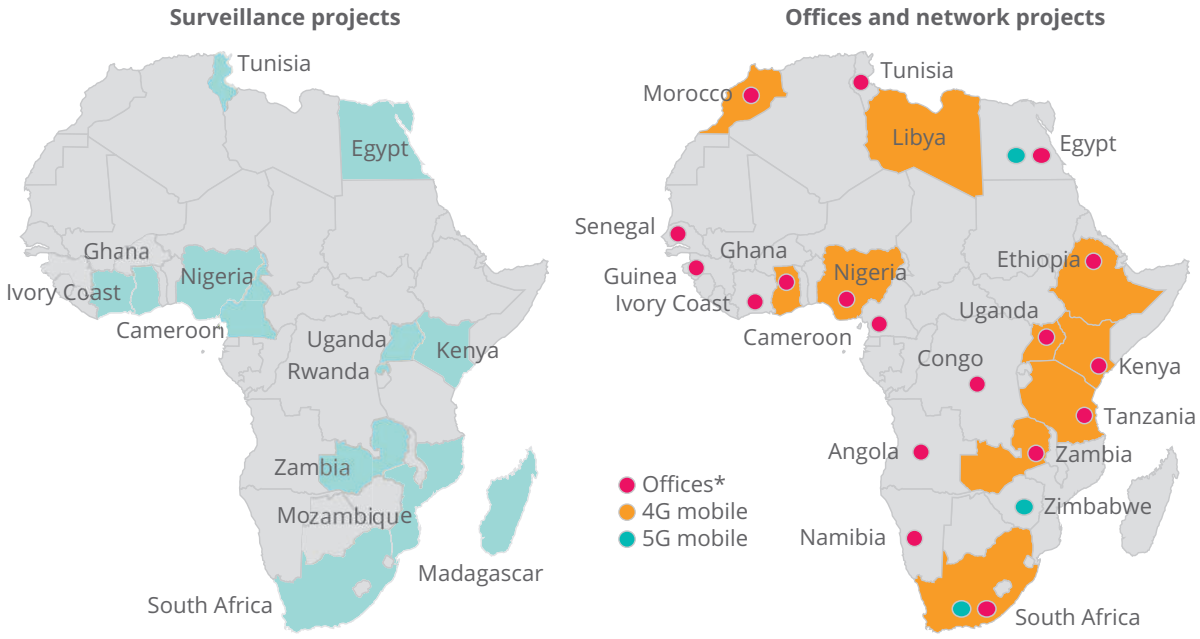



Data compiled by RWR Advisory Group, a Washington-based research firm that tracks Chinese investments abroad. Only projects completed or initiated outside China since 2012 that involve the sale or installation of telecommunications equipment or technology to enhance the digital infrastructure of the target country have been included. As RWR research reflects what has been publically reported, errors and omissions are possible.

**Map 8** | Huawei's Footprint in Africa, 2019[243]

**Continental Drift**

Huawei is Africa's dominant supplier of mobile internet networks and state surveillance systems.




**Smart Cities and Surveillance:** Huawei has connected hundreds of millions of African consumers since first doing business in Kenya in 1998. It has deployed telecom networks in some 40 African nations by brokering low-interest loans and by offering on-the-ground know-how.[244] Huawei, which now controls substantial parts of Africa's internet business, has recently started exporting digital-surveillance systems.

In April 2019, the Chinese government extended a $172 million concessional loan for the construction of a smart city in Kenya called the Konza Technology City. The new development will feature a surveillance system and National Cloud Data Centre, all to be built by Huawei.[245]

Since 2016 in Zambia, Huawei has led the construction of an information and communication technologies training hub and hundreds of cell phone and data connection towers. Huawei has also established a $75 million data centre complex which houses a Cybercrime Crack Squad staffed with a critical mass of Huawei employees.[246]

In May 2018, Uganda's government signed a $126 million deal with Huawei for a safe-cities project, including a digital surveillance unit at Kampala's police headquarters and webs of hundreds of street cameras. Concerns are rising that "safe cities" projects in several countries in North and Sub-Saharan Africa could become hubs of "survival surveillance strategies" used by incumbent regimes to consolidate power.[247]

In this context, technicians from the Chinese telecom, Huawei, have directly used their know-how and tools to help the governments of Uganda and Zambia spying on their political opponents, "including intercepting their encrypted communications and social media, and using cell data to track their whereabouts," according to an in-depth investigation by the Wall Street Journal. The investigation unveils the sophisticated surveillance systems that Huawei sells to governments, often branded "safe cities."[248]

The deployment of critical information infrastructure along China's digital Silk Road has the potential to gradually exclude U.S. technological influence in North- and Sub-Saharan Africa, raising Western concerns about monitoring and interception of critical financial and security data-flows. Such control over transnational digital services, including massive pop-

ulation and consumption data, could give Chinese tech sectors more power to shape BRI markets.

Yet, the battle of influence is not only economic but also normative. Africa's geostrategic importance to China is about a long-term engagement to recruit foreign governments that will align with Chinese illiberal biopolitics methods and norms of governance in cyberspace.

## Cognitive-Emotional Conflicts Waged by Russia

Most of the conflicts that drive the web and the world will have strategic clashes in Africa. After a long period of disinterest in the continent, Russia's government is now trying to rival China's systematic geopolitical positioning in regions that have many data- and resources-reservoirs to exploit in the digital economy. The below map shows that Russia's interest in countries like Nigeria, South Africa and Zimbabwe could step on the territories and markets already engaged through China' s Belt and Road Initiative. (Map 9)

Leaked documents obtained by the Dossier Centre, a research unit based in London unveils Russia's recent attempt at deploying its presence in at least 13 countries across Africa, including Cameroon, Libya, Madagascar, Mozambique, South Africa and Sudan.[249] Russia' strategy includes developing strong ties with ruling governments and political elites, augmenting military presence through arms deals, and nurturing influencers from the African diaspora to turn them into potential leaders and promoters of Russia's interests. Russia's government has already struck military cooperation agreements with about 20 African states and has deployed security and military intelligence presence in the Central African Republic, which is seen as an extremely weak state with lucrative mineral resources. In Africa, Russia's most obvious and successful interference targeted the far-away island of Madagascar.[250] The operation was orchestrated for the Kremlin by Russian agents linked to Yevgeny Prigozhin, the oligarch accused of interfering in the U.S. 2016 elections.

During the influence campaign in Madagascar, Russian operators produced and distributed their own

> "Most of the conflicts that drive the web and the world will have strategic clashes in Africa.

newspapers in the local language, recruited bloggers to write propaganda in favour of the incumbent president, covered billboards with advertisement, bought airtime on TV stations, and even offered bribes to involve a pastor into the presidential race.

The goal of keeping Madagascar's incumbent President in power, however, backfired forcing the Russian operation to rally around the opposing candidate on the eve of the election. In doing so this last-minute opportunistic support achieved the longer-term goal of the operation securing control over a large chromium mining industry.

Other planned electoral operations included supporting incumbent Presidents in Sudan and South Africa with a similar playbook of buying the influence of local journalists and disseminating propaganda news articles and videos.

What seems a growing trend is the ability of Russian operators to generate information disorders through social media campaigns running on African networks.

**Map 9** | Countries Targeted by Russian Interference[251]

Facebook recently announced that it removed three massive influence campaigns led by Russia but operated by local media groups and bloggers-for-hire.[252] The volume of these campaigns was impressive with 8,900 Facebook posts published in October 2019 alone by one node of the African networks.

> What seems a growing trend is the ability of Russian operators to generate information disorders through social media campaigns running on African networks.

Recent reports by CNN journalist, Clarissa Ward and her team, shows that the Kremlin is increasingly outsourcing its information operations to Africa, in particular in Ghana and Nigeria.[253] Cyber mercenaries in those two countries have developed relatively sophisticated influence campaigns aimed at African Americans ahead of the U.S. 2020 elections. Once again and as witnessed in information disorders waged in Kenya and Nigeria, the strategy is to inflame racial and socio-economic tensions with the goal to foment social unrest and de-mobilize segments of the electorate. Increasingly, foreign interference operations exploit African information spheres both as a testbed and strategic stronghold.

In general, Russia's engagement with African nations lacks a coordinated global strategy with long-term financial investment and infrastructure-building. Yet, Russia brings along a vast experience of surveillance and digital manipulation for waging instability in far-away societies. Through its history, the country has mastered the art of manufacturing cognitive-emotional conflicts: tech-driven propaganda aimed at generating political and social disruptions, influencing populations' perceptions, sowing polarization and distrust. Waging trust-deficit disorders is corrosive, particularly when it leads to destroying confidence in the relevance of global financial and governance institutions, from the United Nations, the World Health Organization to the multilateral order itself.

While cognitive-emotional conflicts often entail the instrumentalization of social media, subsequent phases increasingly target important elements of human and civilian security, including beliefs, discourses, digital systems and infrastructures critical to health, food, political, and economic security. In the spring of 2020, as the world is grasping with the dramatic ramifications of a global pandemic, Russia is exploiting its deception playbook to manufacture and spread distrust in governments' ability to fight the viral threat.[254] What is under Russian attack is social cohesion. The resilience of nations and political institutions ultimately lie in the minds of its citizens who today are under constant pressure.

In Africa, Russia's ultimate strategy is slowly resembling this of China with the goals to augment control over the transnational information roads of cyberspace, undermine western influence in Africa, win the interests of established African elites and capture resources along the way.

For state actors in several African nations, Russia's deception machine is appealing as it provides the tools and expertise to manipulate public opinion, lessen populations' political agency, and strengthen regime stability. This collusion of interests between Russian and African political leaders will impact future models of governance and hegemony in cyberspace.

> Foreign interference operations exploit African information spheres both as a testbed and strategic stronghold.

## Tensions at the UN around Normative Leadership

At the renowned World Economic Forum in Davos in January 2019, international leaders from Japan, Germany, South Africa and China called for greater regulatory supervision over the converging technologies and global supply chains that power the digital economy.[255]

While Western governments failed to present a robust, coordinated approach to governance, China's message voiced by Vice President Wang Qishan emphasized the need "to respect the independent

> What is under Russian attack is social cohesion.

choices of model technology management and of public policies made by countries, and their right to participate in the global technological governance system as equals." He even insisted on respecting "national sovereignty and refrain from seeking technological hegemony, interfering in other countries' domestic affairs and conducting, shielding or protecting technology-enabled activities that undermine other countries' national security." President Cyril Ramaphosa of South Africa focused on the need for standards and oversight, specifically to prevent cybercrime and reinforce cybersecurity.

Cyberspace has become not only a new domain of fierce competition over information, business, and strategic technological operations, but also a new battlefield for projecting or undermining normative influence.

Since the end of the cold war, the UN has served as the prevailing multilateral forum to negotiate technological standards and human rights oversight. Standard-setting is crucial as it gives companies a competitive advantage in the market by aligning global rules with the specifications of their own proprietary technology. While Western nations have their own regional standard-setting bodies, companies in developing countries tend to turn for vetting and guidance to the UN's International Telecommunication Union (ITU).

The risk is for the ITU in particular, and the UN in general, to be instrumentalized by tech-leading nations to accept their standards and therefore entrench their competitive advantage and subsequent control over converging technologies. An investigation by the Financial Times reports that China could be exerting this type of lobbying inside ITU by proposing the ratification of new standards for AI technologies, including facial-recognition coupled with CCTV circuit monitoring and other smart city surveillance technologies.[256] Lacking resources to develop and lobby for their own standards, emerging African technological powers are likely to accept the technical and normative specifications agreed upon at the ITU.

Universal standards can have powerful ramifications when shaping the path of intrusive technologies like facial-recognition used in smart policing, criminal justice, and monitoring of public spaces from schools, airports, hospitals to safe cities.

The hard truth is that if the concerns of a critical mass of civil society organizations and human rights defenders are not considered by the ITU, China's private sector leaders could use standard-setting to normalize surveillance technologies within new markets across Africa.

Another form of state-influence at the UN is through discursive power, the potential to reshape the legitimacy of multilateral regulatory tools. The recent series of votes over a UN Cybercrime resolution sponsored by Russia and China provides an excellent example.

In 2019, emerging technological powers – including, Singapore, India, Kenya, Nigeria and South Africa – voted "yes" to support a resolution led by Russia and China, paving the way towards a new global cybercrime treaty. On November 18, the UN cybercrime resolution passed 88-58 with 34 abstentions and 12 no votes. On December 27, countries in favour of the resolution won final approval. With this last vote, the UN assembly decided to establish an open-ended ad-hoc intergovernmental committee of experts representing all regions to elaborate a comprehensive international convention on countering the use of ICT for criminal purposes.

> Cyberspace has become a new battlefield for projecting or undermining normative influence.

Following the vote, the representative of China stressed that "the proposed convention would fill a legal vacuum, benefit developing countries and guarantee inclusiveness in future negotiations."[257] Interestingly, the countries that either sponsored or voted "yes" to the cybercrime resolution nearly overlay the countries that are partners in the BRI initiative (Maps 10 & 6).

The proposed treaty is presented as a more global and inclusive alternative to the US-led Budapest Convention, which ratified in 2011aimed to support

nascent forms of international cooperation, including trans-border data-flows, to counter cybercrime and close the cyber-enforcement gap. Yet, the Budapest Convention was never endorsed by Russia and China.

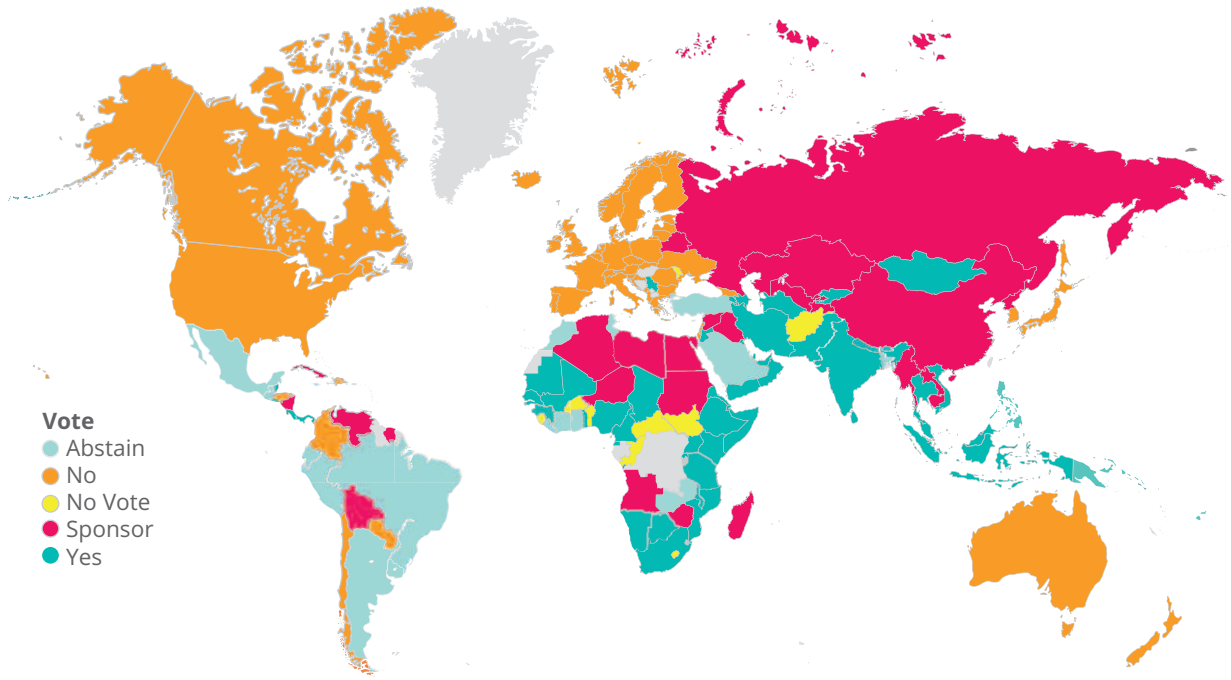
Being able to access data and evidence across borders remains a critical step in cybercrime investigations and prosecutions. Yet, from Russia's and China's perspectives, the Budapest Convention raises important national sovereignty concerns over trans-border access to information and electronic evidence. In particular, Article 32(b) permits states to obtain information in another country without needing this country's government approval if the lawful owner of the data gives consent.

From the Western perspective, at the heart of this new cybercrime resolution is an effort to establish UN-approved global norms that endorse national sovereignty over cyberspace. Such a move could duplicate, dilute, and hamper existing UN initiatives and international collaborations that already support global cyber-enforcement. A gradual balkanisation of cyberspace could even provide criminals with safe-havens from where to perpetrate cybercrimes with more impunity.

Not only that, but the normative vision proposed by Russia and China – which strategically omits to define "cybercrime" – could also be used to impose state control of the Internet, to criminalise legitimate forms of online expression and uses of secure digital communications, as well as to justify surveillance and repression of civil society in authoritarian countries. "A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world," as stressed by the 2019 report of the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association.[259]

By influencing technical standards and global norms, China's diplomatic efforts at the UN also aim to defend a form of cyber-nationalism that normalizes pervasive digital surveillance and new forms of political and social control. As discussed in section IV and V, Beijing seems to be exporting its model of cyber-biopower to other nations, particularly developing and emerging economies in Africa and South-East Asia. For example, Thailand and Vietnam have adopted a similar approach to the Great Firewall – relying on a combination of legislative and

**Map 10** | Vote on the UN Resolution Countering the Use of Information and Communication Technologies for Criminal Purposes (2019)[258]



> A gradual balkanisation of cyberspace could even provide criminals with safe-havens from where to perpetrate cybercrimes with more impunity.

technological tools to regulate the internet domestically. In the wake, Kenya, Ethiopia, Egypt, Algeria, Tanzania, Uganda, Zambia, Zimbabwe and South Africa have imported or are in the process of deploying China's surveillance technologies.

The consequences of these approaches to precision surveillance could be harmful and destructive, potentially leading to violations of human rights, freedom of expression, individual privacy and political agency. The capacity for states to exploit converging technologies for imposing political and behavioural control could make it increasingly difficult, if not impossible, for the UN to monitor and consistently protect against human right violations in regions that lack robust legal protections.

The ultimate goal of Russia's diplomatic engagement at the UN is less systematic and clear but it consists partially, in preserving enough state control to develop and experiment with surveillance technologies that are strategic when waging information warfare, election-shaping operations, and cognitive-emotional conflicts. In November 2019, the Russian government passed a 'sovereign Internet' law which allows it to shut Internet traffic from outside Russia in the context of 'emergencies' and to compel Internet service providers to use software that can filter and reroute traffic.[260] Using computational, diplomatic and legal tools, Russia is carving up cyberspace into its own national cyber-domain.

This national effort aligns with the Russian sponsored UN resolution on a global cybercrime treaty, and its distinct lack of a definition of what cybercrime is and how digital technologies can be misused for criminal purposes. Such strategic omission creates legal uncertainty that can be harnessed to bypass international human rights law and criminalize the online behaviours of civil society, media, public, and corporate actors.

© UN Photo/Isaac Billy

# CONCLUSION: AFRICA'S GEOPOLITICAL FUTURE, EMPOWERING POPULATIONS AND THE ROLE OF THE UNITED NATIONS

The modern internet is not just a set of wires, but a complex ecosystem where billions of digital bodies and minds interact and share data. This expanding digital common bears exceptional economic promises through global and national economic growth and provides empowerment for populations across the globe. Yet, cyberspace is also increasingly an existential threat to democratic processes when it foments violence and amplifies hate speech, falsehoods and terrorist propaganda. In the West, but also in several countries in Africa, information disorders have erupted as new powerful vectors to interfere in elections, undermining citizens' political agency and self-determination. Such emotional wars (cognitive-emotional campaigns) exploit populations' data to deploy new forms of political and behavioural engineering in elections. The potential for large-scale mobilization of people and resources around false narratives creates significant risks to civilian security.

Within the internet of bodies and minds, vast amounts of populations' data are exploited by corporations through aggressive commercial data-mining and profiling, but also by states through technological networks of surveillance justified by securitization agendas. In several African nations, surveillance technologies are co-opted by ruling political elites for real-world electoral impact. In a vicious circle, the convergence of AI and data-capture technologies is harnessed by state-power, not only for manipulating populations' behaviours in elections, but also for strengthening regimes of pervasive information control and repression. This is the postmodern version of Foucault's biopolitics or biopower. Under a form of digital authoritarianism, states preserve regime stability and legitimacy through controlling populations' data and spheres of information.

> "In several countries in Africa, information disorders have erupted as new powerful vectors to interfere in elections, undermining citizens' political agency and self-determination.

Under the same impulse, cyberspace has become not only a new domain of fierce competition over information, business, and strategic technological operations, but also a new battlefield, where adversaries interfere more directly than ever with a targeted nation's political processes and the minds of its citizens. Conflict now opposes societies and competing ideological systems, not just armies. Governments across the world are only starting to realize how the manipulation and weaponization of converging and connected technologies in cyberspace can threaten their attempts to preserve trust, collective security, political and social resilience.

> "Conflict now opposes societies and competing ideological systems, not just armies.

And indeed, ruling governments in Africa increasingly see the back side of the digital economy: its potential to threaten regime stability. They may therefore align with China's vision of reasserting sovereign power over spheres of information. China's cyber-sovereignty model provides an illusion of proactive, tactical methods to benefit from the digital economy, manage external threats, mitigate cybercrime, and control disinformation campaigns, while offering new means to censor public opinion and curtail large-scale demonstrations.

In this battle for normative influence, there is a rising competition between tech-leading nations to exploit the African continent as a geostrategic positioning for controlling populations' data-flows, converging technologies and the underpinning transnational, information infrastructure that ensure economic and security supremacy. The race between US and

> Ruling governments in Africa increasingly see the back side of the digital economy: its potential to threaten regime stability.

Chinese digital platforms to carve territorial hotspots where to build data-centres and 5G networks mirrors a race to impose technical standards for emerging technologies in cyberspace.

How does this multipolar competition impact African nations' effort to carve autonomy and leverage alliances in cyberspace? **And how will this competition impact the role of institutions like the African Union and the United Nations, for instance when threats' mitigation requires global data-sharing particularly in such areas as climate change and pandemics?**

Facing cyber-insecurity around their emerging digital infrastructure, most African nations are also suffering of institutional and regulatory frailty, leaving populations largely vulnerable to data-predation and exploitation by foreign corporate actors or ruling political elites. What is the balance between individual rights and state-command of collective security and prosperity in the digital economy? Policymakers across the world face this question, but in several African countries, where large-scale population data-optimization projects have started in a context of innovation void of any accountability mechanism, it is being posed with urgency.

## Signals from the African Union: Securitization and Surveillance-based Postures

In the last five years, the African Union (AU) and several nations on the continent have used governance efforts to enforce a securitization agenda, raising concerns and resistance of civil society organisations and human rights defenders.

In June 2014, the African Union adopted its Convention on Cybersecurity and Personal Data Protection.[261] This convention establishes a regulatory framework for conducting electronic commerce, ensuring personal data-security, promoting cybersecurity, and addressing cybercrime. While it is crucial for African states to exert leadership in protecting their populations from cybercrime and illegal or harmful online content, such normative leadership may have covert and harmful ramifications for individuals' privacy and freedom of expression. For substantial parts of the global population using internet, state censorship has increased in the last decade. Although the African Union and its Members already committed to good governance in the AU Charter on Democracy, Elections and Governance, the aforementioned AU Convention fails at protecting populations from preying of states and corporations on their data. Not only has a substantial number of African states, including Kenya, Nigeria and South Africa not ratified the Convention over sovereignty concerns, the legal initiative comes with disconcerting implications for human rights.

In the wake, several African nations – South Africa, Kenya, Madagascar, Mauritania, Morocco, Tanzania, Tunisia and Uganda – have enacted or proposed domestic cybersecurity legislation. As explained in section IV and V, some of these legislative efforts present their own threats to data, protection, freedom of expression, and human rights in general.

States have legitimate security and law enforcement rationales for accessing data, but individual citizens should be allowed to question the extent to which personal information can be exploited for rising forms of political and social control.

Another signal coming from the African Union is the three-year memorandum of understanding it signed with Huawei in May 2019.[262] The Chinese telecom giant will partner with the African Union to support capacity-building in an array of sectors, including internet of things, cloud computing, 5G networks and AI, all converging technologies crucial to the Internet of Bodies and Minds and potential securitization agendas. Such cooperation will no doubt be an opportunity to strengthen emerging governance models that might normalize surveillance and place collective security and state preservation over individuals' rights.

Across countries in Africa, where populations' data sets and emerging e-service markets are coveted by technology giants, the battle for data protection and digital rights is the new civil society's fight on the continent.

In a world in which states and corporations increasingly partner to control populations' behaviours and their information networks, how can the United Nations provide normative leadership to help promote populations' data protection and therefore protect human rights? In particular, is there a role for UN agencies to tailor such normative leadership to prevent the rising forms of political manipulation that impact populations through information disorders and electoral disruptions?

The resurgence of cyber-nationalist agendas across the world, including in Africa, points to a dwindling capacity of the multilateral system to play a meaningful role in the global governance of cyberspace. Some corporations may see little value in bringing multilateral approaches to the deployment of lucrative and proprietary technologies that form the "Biometrics and Surveillance Assemblage." Some Member States may prefer to crystallize their own competitive advantages through gaining early access to Africa's massive data-markets. They may instrumentalize United Nations involvement in standard-setting efforts to entrench their own control over 5G networks and converging technologies.

But there are some innovative ways in which the United Nations can help build the kind of collaborative, transparent networks that may begin to address our "trust-deficit disorder". First, the United Nations should strengthen its relationship with the African Union and the African Commission on Human and Peoples' Rights (ACHPR) as closer collaboration could support the basis for further normative leadership. In September 2019, the UN Human Rights Council (OHCHR) and ACHPR signed a formal agreement with the goal to consolidate and improve human rights, including digital rights, across the African continent.[263] Given the powerful implications that AI, biometrics, digital ID systems and surveillance technologies may have for privacy, political agency and other individual freedoms, OHCHR and ACHPR will need to monitor and guarantee coherence across multiple normative efforts spurred by national, regional and private actors.

Second, the United Nations should not only strengthen its engagement with the large technology platforms investing in Africa's digital future, but strongly support truly meaningful cooperation between them, along with civil society actors and member states. In several countries in Africa, civil society organisations have been the main voice and instrument of resistance when populations' data were abused and digital rights violated.

"Across countries in Africa, the battle for data protection and digital rights is the new civil society's fight on the continent.

In a 2019 UNU report, the author proposed to equip the UN with a global foresight observatory, which would develop a responsible governance approach to harness AI and converging technologies for the prevention agenda and for social empowerment.[264] This global observatory could foster tailored collaboration to support civil society organisations, digital rights labs and young innovators in Africa in their effort to build digital governance models that meet the ethical needs of African populations.

In this brokering function, an array of entities within the United Nations system could play a role that is sorely needed at the international level: 1) support to negotiate adequate normative frameworks for populations' data-protection, privacy and digital rights; 2) normative foresight to better implement data-protection mechanisms, which are tailored to African countries' challenges; and 3) the development of strategic monitoring and crisis planning capacity for electoral management bodies to help mitigate the impact of information disorders in elections.

> Facing cyber-insecurity around their emerging digital infrastructure, most African nations are also suffering of institutional and regulatory frailty, leaving populations largely vulnerable to data-predation.

## Normative Leadership & Data Protection in Elections

Section II describes the far-reaching and rapid deployment of Africa's Internet of Bodies and Minds. Across Africa, societies are about to face an unprecedented upheaval powered by the integration of AI and data-optimization technologies into politics, daily life and elections.

To be eligible for essential public services from healthcare, food allowance, welfare to un-employment subsidies and internet access, individuals in Kenya, Nigeria, South-Africa, Tanzania, and Ghana need to register their fingerprints, facial and iris scans. Digital ID systems create an interdependence between our digital behaviours, our ethnic background, our lives and identity offline. As eloquently said by Wafa Ben-Hassine, from Access Now, "this digital identity can then become the target of exploitation, either for commercial or political ends."[265]

© UN Photo/Logan Abassi

Implications for populations' privacy and agency could be corrosive. State and private sector actors engaged in shaping the political regimes of African nations could exploit the combination of AI and populations' sensitive information to exert new forms of political, social and behavioural engineering. Equipped with the technological tools to analyse and control how humans act upon information and knowledge, government and corporations involved in Africa's elections can increasingly monitor and influence populations' attitudes with the drastic potential to manipulate and restrict political agency.

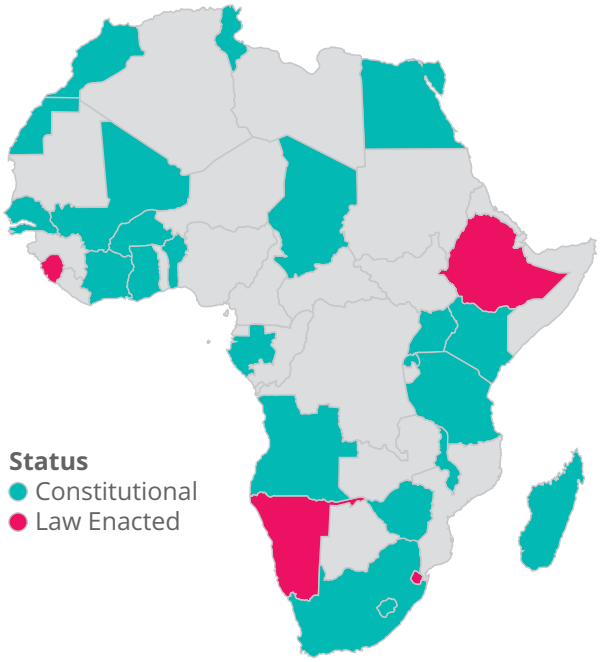
In 2020, 24 African countries out of 53 are in the process of adopting or updating laws and regulations to protect citizens' personal data. (Map 11)

In Kenya and several countries across Africa, emerging normative efforts focused on personal data protection are in direct tension with the rapid adoption of biometric ID and voting registration, at a speed that outpaces legitimate, meaningful policy-making. The risk is that governments will pass inadequate data protection law in haste without proper consultation or input by civil society. As shown in section II-IV, laws developed without enough public scrutiny and inputs from diverse stakeholders, including voices from civil society, are putting marginalized populations at risk of serious human rights abuses.

This tension will have decisive implications for the numerous elections to come in 2020 and 2021. At least, 30 African nations will go to the polls, for both legislative and presidential elections. These include Ghana, Ethiopia, the Central African Republic as well as countries in the Sahel that face increasing instability, terrorist threats, migrations and potential Russian interference in elections. Authoritarian regimes in Egypt, Burundi, Tanzania will have elections in 2020 and Uganda and Zambia in 2021. (Map 1)

Citizens in the majority of these countries will rely on biometrics voter registers, which create significant vulnerability when handling their personal data: thousands of employees and many offices can access databases; foreign technological vendors are

**Map 11** | National Data Protection Law[266]




involved for key technical functions; cybersecurity protection are not often adequate; and data-protection authorities might not have the discretion and capacity to oversee complex supply chains and proprietary technologies. One cybersecurity expert testifying in front of Kenya's hight court explained that the biometric program would be vulnerable to hacking, creating pervasive risks that Kenya's government did not have the technological expertise to mitigate.[267]

Biometrics ID systems may also expose populations to privacy breaches if they are not clearly defining and respecting rules that ensure purpose limitations, data quality, transparency, and restrictions for third-party access and cross-border data-transfers. Another major source of privacy and security uncertainty comes with the conditions for biometric data-storage: individuals' biometric data might be stored in cloud computing servers, potentially outside of the country of origin.

> In several countries in Africa, civil society organisations have been the main voice and instrument of resistance when populations' data were abused and digital rights violated.

In the absence of adequate laws, policies, and corporate practices that are grounded in internationally recognized principles for human rights, the most intimate data we share can be used to undermine democratic processes and hurt the most vulnerable among us.

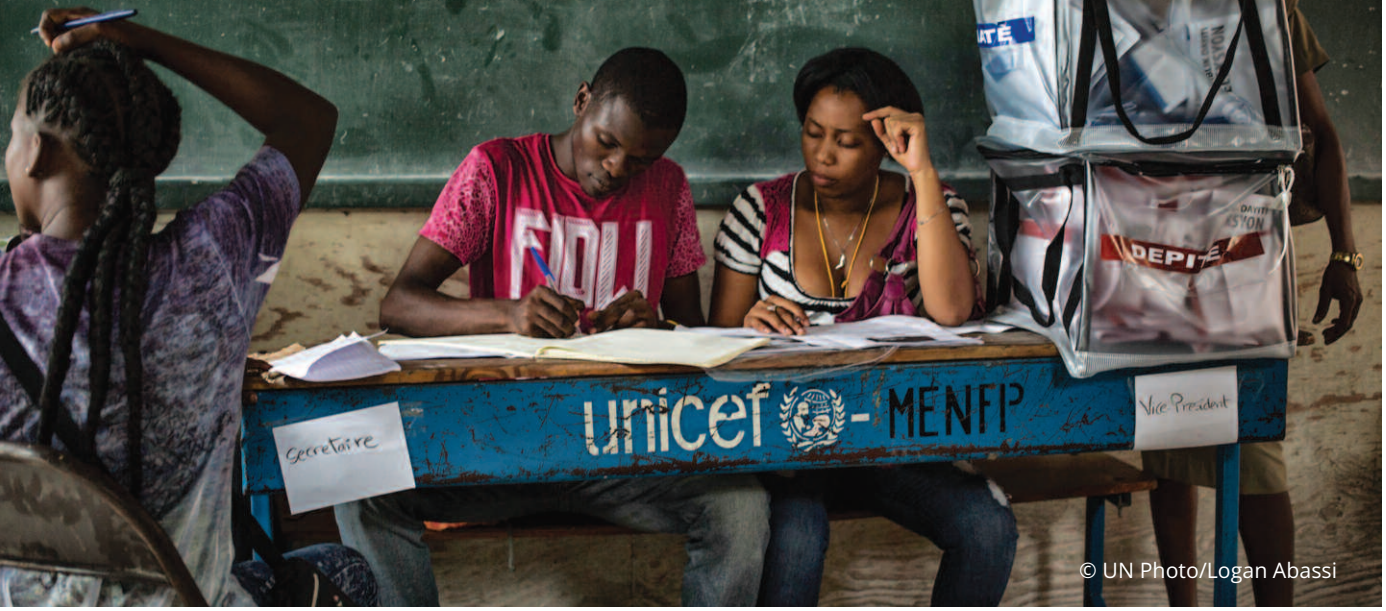
A timely and crucial diagnosis is that, in the race to achieve the promises of the digital economy, we face a pervasive, harmful gap between our normative frameworks and the implementation of meaningful accountability. This is essentially a failure, an incapacity to translate high-level ethical declarations into viable normative mechanisms that can ensure meaningful accountability, for an array of populations, with their particular vulnerabilities, but also their normative preferences.

> In the race to achieve the promises of the digital economy, we face a pervasive, harmful gap between our normative frameworks and the implementation of meaningful accountability.

In the corporate ecosystem, the UN Guiding Principles on Business and Human Rights are supposed to support that normative translation, but lack strong incentives for and proactive engagement from corporations. In truth, what we slowly realize are the serious limits of self-regulation to produce accountability for all.

This is where the African Union and the UN could play a unique role in normative leadership, including by strengthening the role and reach of the UN Guiding Principles on Business and Human Rights.

Both institutions, the United Nations and the African Union, could provide a forum where public and private sector actors, in collaboration with civil society, can work together to translate high-level principles of personal data protection laws into operational



© UN Photo/Logan Abassi

> As data protection laws emerge in countries in Africa, governments might impose tighter national control of the internet, for instance by adopting China's data-localization principles, requesting data to be stored in the country of origin.

mechanisms and practices. They will also need to stress-test these normative practices in the context of different scenarios where privacy could be breached and personal data abused, resulting in human right violations.

In 2019, Kenya passed its first Data Protection Act[268]while Nigeria issued a substantive set of Data Protection Regulations.[269] For both, the 2016 EU GDPR offers inspiration on high-level privacy principles and limited guidance on how to translate these principles into operational normative mechanisms that will ensure both, transparency and accountability. Another crucial test will be whether newly formed data protection authorities in Kenya and Nigeria will have the required independence to scrutinize and, if necessary, impose fines on powerful state agencies or private corporations that would exploit and abuse populations' data. There are also concerns as to whether the new data protection authorities will have the capacity to manage all of their responsibilities with very limited legal precedent to use for guidance. As, both countries progressively strengthen their regulatory capacity, this normative effort is a significant first step towards responsible data-governance.

In this debate about data protection, a rising concern for policymakers, diplomats and, more importantly, CEOs with global reach, is the risk to face increasing competing visions of governance and a balkanization of cyberspace with diverging standards on privacy, security, free speech, and cross-border data-transfers. As data protection laws emerge in countries in Africa, governments might impose tighter national control of the internet, for instance by adopting China's data-localization principles, requesting data to be stored in the country of origin. This is why we currently witness a race between U.S. and Chinese technological platforms to build data centres and information infrastructures on strategic territories – coastal cities and resource-hotspots – in African countries.

Such regulatory move towards data-localization and cyber-sovereignty would make it increasingly difficult for the United Nations and its agencies (like the World Health Organisation) to rely on global data-sharing to address shared problems such as mitigating the dramatic consequences of a pandemics. This is another complex governance problem, which the United Nations will have to manage if the institution wants to stay relevant when it comes to prevention and development.

In the near-future, tech-leading nations and their corporate partners will increasingly instrumentalise the UN mandate in normative and technical capacity-building to crystallize their competitive advantage

> This era of information disorders and "emotion wars" strongly affect trust in the multilateral order and in the UN leadership to protect global populations from technological and biological threats.

(through standards and proprietary technologies) and augment their control over transnational cyberspace infrastructures.

Beyond the internet of bodies and minds, states' competition is also about amplifying spheres of normative influence through discursive power and the cyber-stories they tell. The race for showing governance leadership, through narratives and actions, was clear during the pandemics that erupted in 2020. China, for instance, tried to eclipse foreign fears and resentment about the dramatic global impact of Covid-19 with medical equipment sent to European countries that were too burdened to share supplies within their internal market's borders. Inland, videos of hospitals built in haste provided virtual consolation to China's affected populations.

The UN will not be immune to rising attempts at using discursive power and information disorders to weaken the traditional values of multilateralism.

This era of information disorders and "emotion wars" strongly affect trust in the multilateral order and in the UN leadership to protect global populations from technological and biological threats, form surveillance, digital and epistemic manipulation.

For the UN, the only way ahead to preserve relevance is to work with member states to shape and exert forward-looking and robust normative guidance, partnering with the next-generation of civil society and private sector actors to empower populations across the world. We need visionary normative leadership.

Existing and future technological inequalities, not only in capacity-building but in prevention, will be significant in determining who flourishes and who fails in the converging technological future. Institutional and regulatory frailty is another problem in a fast-pace digital economy. At the same time, a complex understanding of converging technological and information risks does not underpin global development strategies.

Whose duty is it to foresee the unintended consequences of dual-use, converging technologies on our societies and who possesses the required expertise for preventing harm? To meet these challenges, we need a common understanding of emerging information and security risks across the international community, driven by incentives for a shared approach to prevention.

Though the goal is ambitious, it is the only way to shape technological convergence so that it empowers vulnerable populations, protects human rights, and meets the ethical needs of a digitalizing and globalizing world.

© Unsplash/Lagos, Nigeria

# FUTURE RESEARCH AGENDA AND PRACTICAL RECOMMENDATIONS

Section II-III provides an in-depth analysis of the anatomy of information disorders in selected African countries. One of the major trends identified is the increasing capacity and willingness of ruling governments in Africa to instrumentalize digital networks for inflaming existing racial, social and economic tensions between sub-populations. In countries where privacy and data protection laws are not translated into robust operational mechanisms, state and private sector actors can extract sensitive personal data from an array of online population databases for targeting ethnic and socio-economic groups.

These emotion wars can be orchestrated by political parties themselves or crafted by the foreign data-analytics companies they hire within lucrative contracts. Information disorders have had powerful ramifications in an array of nations, including in the UK and U.S., sowing distrust and polarization. But, populations in Africa that have suffered recent or long-lasting violent crises, are particularly vulnerable to political and social engineering through the weaponization of social media.

**Strategic Crisis and Scenario Planning with Electoral Management Bodies (EMBs):** EMBs could collaborate closely with UN's electoral assistance experts in monitoring information disorders and overseeing populations' data protection mechanisms during election periods. In a 2019 report on Social Media, Disinformation and Electoral Integrity, IFES proposed to use methods of crisis and scenario planning to support EMBs in anticipating the nature and scope of disinformation threats and better plan disinformation responses.[270] IFES experts stress the potential of using crisis simulation models – such as table-top exercises – to assist EMBs build threats and solution scenarios in real-time and develop resilience responses to disinformation campaigns.[271] Collaboration between EMBs, UN electoral assistance experts and social media companies could be extremely useful in designing such matrices for assessing vulnerabilities and threats and plan reaction strategies tailored to the specific anatomy of information disorders in an African country.

In the context of crisis and scenario planning, EMBs could make use of social media monitoring tools to identify specific demographic subgroups and social divisions vulnerable to exploitation by disinformation actors. Another crucial measure for EMBs would be to better anticipate how to enhance the security of biometrics and digital ID registration infrastructures to prevent exfiltration and exploitation of voters' sensitive data in disinformation. In this effort to prevent political and behavioural engineering targeted at specific population subgroups, collaboration with civil society and private sector actors would be instrumental.

Two recent examples of cooperation between civil society organisations, traditional media and social media companies could be extended to include strategic crisis monitoring and scenario planning with EMBs. Prior to Nigeria's 2019 elections, local civil society groups provided vital expertise and contextualised knowledge to support Facebook in fact-checking and limiting the spread of disinformation. Facebook has also scaled up a partnership with the rising network of African media experts under Africa Check to monitor mis- and disinformation in 15 sub-Saharan countries, working in local languages – as well as with local news outlets.[272] Such partnerships constitute catalysts for knowledge-sharing which could be harnessed in strategic crisis monitoring and planning.[273]

**Closing the Accountability Gap and Empowering Civil Society:** The German Marshall Fund's Digital Innovation and Democracy Initiative (DIGI) recently published a policy roadmap that favours bottom-up methods to preserve the integrity of our spheres of information.[274] While this roadmap is initially better suited for Western democracies' information ecosystem, several of DIGI proposals

could be tailored to the epistemic challenges faced by African societies.

**Early-detection and mitigation of domestic and foreign digital manipulation campaigns** could be done through agile knowledge- and threat-sharing between large telecommunication and internet platforms; electoral management bodies; independent government agencies; and civil society organisations.

**Fostering transparency and accountability practices** within information spheres could involve close collaboration between social media platforms and civil society actors to develop a code of conduct or "civic contract." But, again, this will only succeed if an independent authority can incentivise transparent data-sharing, compliance and agile oversight.

Foreign and domestic attempts at engineering voters' behaviours have been exposed by multiple movements of resistance, particularly in Kenya and South Africa, where civil society activists, journalist, women's organisations and young thought leaders used social media to organize concurrent virtual spaces for civic debates sharing insights across ethnicities.

A next crucial step would be to create an independent support mechanism to **empower virtual civic spaces** where public-interest journalism, fact-checking, voting information and media literacy can thrive. This is sorely needed in South Africa, but even more in Kenya and Nigeria where dynamics of media capture and censorship are on the rise.

In South Africa, the Independent Electoral Commission, in partnership with Media Monitoring Africa, has launched "Real 411 – Fight Disinformation Together," an online reporting platform for citizens to report cases of alleged digital disinformation.[275] Such an initiative is supported and amplified by the efforts of vibrant media actors such as the Daily Maverick, which has built "disinformation archives" and engaged in long-term investigation on "merchants of disinformation" and "state and media capture." Despite online threats and harassment, often gender-based, journalists in South Africa have used both talent and foresight to help unveil information disorders. Renown author Nyabola describes in her book how feminist activists in Kenya built "We Are 52%," an online resistance movement coupled with powerful offline mobilisation to empower women in public life.[276] Both efforts would benefit from support by the larger information ecosystem and could serve as inspiration for civil society in other countries.

**Multi-stakeholder Research Partnership on Information Disorders and Hate Speech in Elections:** Launched in June 2019, the United Nations Strategy and Plan of Action on Hate Speech stresses the importance of both, leveraging partnership with private sector and civil society actors, to better understand the root causes and drivers of hate speech and information disorders.

What are the socio-technological enablers of online hate speech and information disorders? How can we keep pace with the evolution of these new forms of cognitive-emotional conflicts as technologies combine and amplify each other's effects? The below research agenda aims to provide policy insights for UN entities on how the convergence of technologies for data-mining and digital manipulation will provide opportunities and challenges to addressing hate speech and disinformation.

The combination of converging technologies, from AI, facial recognition, affective computing, and biometrics provides state and non-state actors with more tools to subject populations to new forms of digital manipulation; first, inflaming ethnic and socio-economic tensions, to better exert political and behavioural engineering. Information, elections and conflicts are increasingly entangled. In this context, the UN is needed more than ever as a community of experts, diplomats and policymakers with knowledge and understanding of local, regional and international politics, and as a convening power for entrepreneurs, civil societies, and States, including the most vulnerable ones.

The UN can work with social media companies and AI engineers to help them anticipate and mitigate how technological convergence will be harnessed to manipulate populations and political systems. Entrepreneurs and engineers are currently the main actors shaping what implications AI and converging technologies will have for the conduct of conflict, social cohesion, and human rights. Far from being just neutral information providers, through the use

of their determinative algorithms, social media platforms play a substantial role in enabling the waging of virtual conflicts and their real-world results.

The UN can also support Member States in anticipating and understanding the implications that technological convergence can have in a new geography of virtual conflicts. Such conflict space, with its potential for deception and subversion, will increasingly matter and bear significant consequences to both, national security and citizens' security. In this context, reinforcing the resilience of societies to deceptive digital campaigns is even more complex and deserves urgent attention in conflict studies. One strategic element to remember is that deception thrives on existing vulnerabilities, from economic exclusion, lack of social cohesion, political discord, disengagement or polarization, to cultural, religious and ethnic dissensions.

Experts in preventive diplomacy have developed comprehensive expertise in analysing conflict dynamics, building sensitive political relationships in fractured countries, and conducting "framework diplomacy" with allies to create a safer space for crisis management. These experts are skilled to analyse the internal drivers of recent and current conflicts, to identify likely threats to peace and to anticipate how they may evolve if left unaddressed. This expertise and collaborative practices can be leveraged to better anticipate the nature, depth and scope of social and political vulnerabilities that information disorders, hate speech and technological deception may target.

One strategic option might be to build collaborative teams of civil society and media actors with experts in electoral assistance, preventive diplomacy, conflict resolution and converging technologies. Such a brain-trust could conduct a combined socio-technical systems analysis to 1) identify emerging tensions, anomalies and divisions in fractured societies; 2) anticipate subsequent scenarios of digital manipulation, including hate speech and disinformation; and 3) plan for strategies to rapidly and effectively mitigate information disorders, in particular at crucial election times.

These types of collaborations could serve as a form of early-warning system to help social media and AI technological platforms better understand, detect and mitigate data-manipulation, forgeries, disinformation, targeted propaganda, hate speech and political and behavioural engineering. Such an effort would also help raise general awareness of potential vulnerabilities before and during election times. It could help enter into mediation process with more tactical insights on information disorders, which could be critical in strategic engagement with the parties at stake. It would also benefit larger networks of diplomats and policymakers, journalists and citizens.

Anticipating both, the internal and external tensions that influence internationalized civil wars, and understanding how, in this context, domestic and foreign actors could harness digital manipulation, is likely to be a recurrent prevention challenge for regional players and multilateral organisations in the years ahead.

# References


1 Ward C., Polglase K., Shukla S., Mezzofiore G., and Lister T., 2020. "Russian election meddling is back -- via Ghana and Nigeria -- and in your feeds". *CNN.* https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html

2 Goel V. and Rahman, SA., 2019. "When Rohingya Refugees Fled to India, Hate on Facebook Followed ". *The New York Times.* https://www.nytimes.com/2019/06/14/technology/facebook-hate-speech-rohingya-india.html

3 Segal D., 2018. "How Bell Pottinger, P.R. Firm for Despots and Rogues, Met Its End in South Africa". *The New York Times.* https://www.nytimes.com/2018/02/04/business/bell-pottinger-guptas-zuma-south-africa.html

4 Nyabola N., 2018. "In Kenya, Election Manipulation Is a Matter of Life and Death". *The Nation.* https://www.thenation.com/article/archive/in-kenya-election-manipulation-is-a-matter-of-life-and-death/ ; See also, Nyabola N., 2019. "Digital Democracy, Analogue Politics: How the Internet Era Is Transforming Politics in Kenya". *Foreign Affairs.* https://www.foreignaffairs.com/reviews/capsule-review/2019-08-12/digital-democracy-analogue-politics-how-internet-era-transforming

5 Cambridge Analytica Ltd (CA) was a British firm operating in the political influence and consultancy business, using combinations of methods such as exfiltration of digital assets, data mining, data brokerage and data analysis to produce strategic intelligence prior and during elections. It was launched in 2013 as an offspring of the strategic intelligence and defence company, the Strategic Communications Laboratories, also called the SCL Group. After closing operations with legal proceedings including bankruptcy, members of the SCL Group have been continuing operations under the legal entity Emerdata Limited. Cambridge Analytica closed operations in 2018 in the course of the Facebook–Cambridge Analytica data scandal, although related firms still exist.

6 The International Foundation for Electoral Systems (IFES) relies on Wardle and Derakhshan (2017) to frame information disorder as a structural phenomenon, including an agent, message, and interpreter, that "contaminates public discourse, working as a pollutant in the information ecosystem." See Wardle C., Derakhshan H., 2017. "Information Disorder: Toward an interdisciplinary framework for research and policymaking". *Council of Europe.* https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c and Martin-Rozumilowicz B., and Kuzel R., 2019. "Social Media, Disinformation and Electoral Integrity". *International Foundation for Electoral Systems.* https://www.ifes.org/sites/default/files/ifes_working_paper_social_media_disinformation_and_electoral_integrity_august_2019_0.pdf

8 Dahir A., 2020. "Kenya's New Digital IDs May Exclude Millions of Minorities". *The New York Times.* https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html

8 Mayhew S., " Ugandan police deploy Gemalto tech for rapid capture of suspects' biometric data". *Biometric Update.* https://www.biometricupdate.com/201902/ugandan-police-deploy-gemalto-tech-for-rapid-capture-of-suspects-biometric-data

9 Source: Biometrics Update; Privacy International

10 Source: Electoral Institute for Sustainable Democracy in Africa

11 Adams R. 2017. "Michel Foucault: Biopolitics and Biopower." Critical Legal Thinking; 10 May. https://criticallegalthinking.com/2017/05/10/michel-foucault-biopolitics-biopower/#fnref-22546-11

12 Building on relative consensus emerging from scholars such as Jack (2017), Wardle and Derakhshan (2017), the MediaWell project provisionally defines *disinformation* as: "a rhetorical strategy that produces and disseminates false or misleading information in a deliberate effort to confuse, influence, harm, mobilize, or demobilize a target audience." As another expression of information disorders, the MediaWell project defines *misinformation* as "false or misleading information, spread unintentionally, that tends to confuse, influence, harm, mobilize, or demobilize an audience." Scholars such as Benkler, Faris, and Roberts (2018) define propaganda as "the intentional manipulation of beliefs," and as "communication designed to manipulate a target population by affecting its beliefs, attitudes, or preferences in order to obtain behavior compliant with political goals of the propagandist" (2018, 6, 29). See Benkler Y., Faris R., and Roberts H., 2018. "Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics" *Oxford University Press.* https://mediawell.ssrc.org/cita-

tion/network-propaganda-manipulation-disinformation-and-radicalization-in-american-politics/ In the United Nations Strategy and Plan of Action on Hate Speech, the term hate speech is understood as "any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor."

13 For a scenario that describes the "Internet of Bodies and Minds," See Pauwels E., 2019. "The New Geopolitics of Converging Risks". United Nations University. https://collections.unu.edu/eserv/UNU:7308/PauwelsAIGeopolitics.pdf

14 Malalo H. and Mohammed O., 2018. "Kenya's president signs cybercrimes law opposed by media rights groups". *Reuters.* https://www.reuters.com/article/us-kenya-lawmaking/kenyas-president-signs-cybercrimes-law-opposed-by-media-rights-groups-idUSKCN1IH1KX

15 Schwirtz M. and Borgia G., 2019. "How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader". *The New York Times.* https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html

16 Cadwalladr C., 2020. "Fresh Cambridge Analytica leak 'shows global manipulation is out of control". *The Guardian.* https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation

17 Privacy International, 2020a. "2020 is a crucial year to fight for data protection in Africa". *Privacy International.* https://www.privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa

18 El Kadi T., 2019. "The Promise and Peril of the Digital Silk Road". *Chatham House.* https://www.chathamhouse.org/expert/comment/promise-and-peril-digital-silk-road

19 Schwirtz M. and Borgia G., 2019.

20 Privacy International, 2020a

21 Pauwels E., 2019. "The New Geopolitics of Converging Risks". United Nations University. https://collections.unu.edu/eserv/UNU:7308/PauwelsAIGeopolitics.pdf

22 Tucker P., 2019. "The West Isn't Ready for the Coming Wave of Chinese Misinformation: Report". *Defense One.* https://www.defenseone.com/technology/2019/03/researcher-west-isnt-ready-coming-wave-chinese-misinformation/155400/

23 Singer P., Wood P., and Stone A., 2020. "How China Is Working to Quarantine the Truth About the Coronavirus". Defense One. https://www.defenseone.com/ideas/2020/02/how-china-working-quarantine-truth-about-coronavirus/162985/

24 Foucault M. The History of Sexuality. An Introduction, Vol. 1. Trans. Robert Hurley. 1976. New York: Vintage Books, 1990: p. 138-139.

25 Mayhew S., " Ugandan police deploy Gemalto tech for rapid capture of suspects' biometric data". *Biometric Update.* https://www.biometricupdate.com/201902/ugandan-police-deploy-gemalto-tech-for-rapid-capture-of-suspects-biometric-data

26 Chutel L., 2018. "China is exporting facial recognition software to Africa, expanding its vast database". *Quartz Africa.* https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

27 Kwet M., 2019. "Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa". *Vice News.* https://www.vice.com/en_us/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa

28 Segal D., 2018.; Moore J., 2018. "Cambridge Analytica Had a Role in Kenya Election, Too". *The New York Times.* https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html

29 Cadwalladr C., 2019. "Cambridge Analytica a year on: 'a lesson in institutional failure". *The Guardian*. https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie

30 Madowo L., 2018. "How Cambridge Analytica poisoned Kenya's democracy". T*he Washington Post.* https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/

31 See note 23

32 Schwirtz M. and Borgia G., 2019.

33 Cadwalladr C., 2020.

34 Cadwalladr C., 2020.

35 Commission of Inquiry into Post-Election Violence (CIPEV), 2018. "Final Report". https://reliefweb.int/sites/reliefweb.int/files/resources/15A00F569813F4D549257607001F459D-Full_Report.pdf

36 Kenya National Commission on Human Rights, 2017. "Alternative Report to the Committee on Elimination of All Forms of Racial Discrimination". https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/KEN/INT_CERD_IFN_KEN_27238_E.pdf

37 Human Rights Watch, 2018. "Kenya- Events of 2017". *HRW.* https://www.hrw.org/world-report/2018/country-chapters/kenya

38 Commission of Inquiry into Post-Election Violence (CIPEV), 2018.

39 Human Rights Watch, 2018.

40 Privacy International, 2018. "Further questions on Cambridge Analytica's involvement in the 2017 Kenyan Elections and Privacy International's investigations". *Privacy International.* https://privacyinternational.org/long-read/1708/further-questions-cambridge-analyticas-involvement-2017-kenyan-elections-and-privacy

41 Muthuri R., Monyango F., and Karanja W., 2018. "Biometric technology, elections, and privacy: Investigating privacy implications of biometric voter registration in Kenya's 2017 Election Process." Centre for Intellectual Property and Information Technology Law. https://www.cipit.org/images/downloads/CIPIT-Elections-and-Biometrics-Report.pdf

42 Dahir A., 2017. "WhatsApp and Facebook are driving Kenya's fake news cycle". *Quartz Africa.* https://qz.com/africa/1033181/whatsapp-and-facebook-are-driving-kenyas-fake-news-cycle-ahead-of-august-elections/

43 Nyabola N., 2017. "Texts, Lies, and Videotape". *Foreign Policy.* https://foreignpolicy.com/2017/08/01/texts-lies-and-videotape-kenya-election-fake-news/

44 https://www.nytimes.com/2017/10/30/world/africa/kenya-election-kenyatta-odinga.html

45 Muthuri R., Monyango F., and Karanja W., 2018; Mutung'u G., 2018. "The Influence Industry Data and Digital Election Campaigning in Kenya". *Tactical Technology Collective.* https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

46 Muthuri R.; Monyango F.; and Karanja, W., 2018.

47 Privacy International, 2017, "Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism In Kenya". *Privacy International.* https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya

48 Privacy International, 2019a. "State of Privacy Kenya". *Privacy International.* https://privacyinternational.org/state-privacy/1005/state-privacy-kenya

49 Freedom House, 2019. "Freedom on the Net 2019- Kenya". *Freedom House.* https://freedomhouse.org/country/kenya/freedom-net/2019

50 National Coalition of Human Rights Defenders of Kenya, 2018. "Stop Watching Me". *Privacy International.* p 12. https://issuu.com/nchrd-k/docs/edited_nchrd_survey_report

51 Dahir A., 2019. "Chinese firms are driving the rise of AI surveillance across Africa". *Quartz Africa.* https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa/

52 Closed-Circuit TV Cameras

53 Bailey N., 2017. "East African States Adopt China's Playbook on Internet Censorship". *Freedom House.* https://freedomhouse.org/article/east-african-states-adopt-chinas-playbook-internet-censorship

54 Bright S., 2017. " After Trump, "big data" firm Cambridge Analytica is now working in Kenya." *BBC.* https://www.bbc.com/news/blogs-trending-40792078 Nyabola N., 2020. "Cambridge Analytica and the end of elections". Al Jazeera. https://www.aljazeera.com/indepth/opinion/cambridge-analytica-elections-200112201424047.html

55 Gross A., Murgia M., and Yang Y., 2019. "Chinese tech groups shaping UN facial recognition standards". *Financial Times.* https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67

56 Dahir A., 2020.

57 Burt C., 2018. "Somaliland election saw Iris ID technology deployed." Biometric Update. https://www.biometricupdate.com/201801/somaliland-election-saw-iris-id-technology-deployed

58 Dahir A., 2020.

59 Mayhew S., 2019. " Ugandan police deploy Gemalto tech for rapid capture of suspects' biometric data". *Biometric Update.* https://www.biometricupdate.com/201902/ugandan-police-deploy-gemalto-tech-for-rapid-capture-of-suspects-biometric-data

60 Madianou M., 2019. "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies". *Television and New Media.* https://journals.sagepub.com/doi/abs/10.1177/1527476419857682

61 Calistra C., 2015. "Emotion Analysis in the Real World". *Kairos.* https://www.kairos.com/blog/emotion-analysis-in-the-real-world

62 Umematsu T., Sano A., and Picard R., 2019. "Daytime Data and LSTM can Forecast Tomorrow's Stress, Health, and Happiness,". *41st International Engineering in Medicine and Biology Conference.* https://www.media.mit.edu/publications/daytime-data-and-lstm-can-forecast-tomorrow-s-stress-health-and-happiness/

63 Halpern S., 2020. "The Neuroscience of Picking a Presidential Candidate. *The New Yorker*. https://www.newyorker.com/tech/annals-of-technology/the-neuroscience-of-picking-a-presidential-candidate

64 Coppins M, 2020. "The Billion-Dollar Disinformation Campaign to Reelect the President". *The Atlantic.* https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/

65 Mosk M., Turner T., and Faulders K., 2018. "Russian influence operation attempted to suppress black vote: Indictment". ABC News. https://abcnews.go.com/Politics/russian-influence-operation-attempted-suppress-black-vote-indictment/story?id=53185084 Etter L., 2017. "What Happens When the Government Uses Facebook as a Weapon?" *Bloomberg Businessweek.* https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook

66 BPU Holdings, 2018. "ZimGo Polling Is First Emotion AI Election Analytics and Forecasting Service for US Campaigns". *BusinessWire.* https://www.businesswire.com/news/home/20180430005331/en/ZimGo-Polling-Emotion-AI-Election-Analytics-Forecasting

67 HaystaqDNA. https://haystaqdna.com/

68 Tactical Tech, 2019. "Personal Data: Political Persuasion Inside the Influence Industry. How it works". *Tactical Tech.* p. 22. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf

69 AI Now Institute, 2019. "AI Now 2019 Report". https://ainowinstitute.org/AI_Now_2019_Report.html

70 Kwet M., 2019. "Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa". *Vice News.* https://www.vice.com/en_us/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa

71 Crawford K., 2019. "Regulate facial-recognition Technology". *Nature.* https://media.nature.com/original/magazine-assets/d41586-019-02514-7/d41586-019-02514-7.pdf

72 Pauwels E., 2019. "The New Geopolitics of Converging Risks". United Nations University. https://collections.unu.edu/eserv/UNU:7308/PauwelsAIGeopolitics.pdf

73 Privacy International, 2020.

74 Mutung'u G., 2018. "The Influence Industry Data and Digital Election Campaigning in Kenya". *Tactical Technology Collective.* https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

75 Itimu K., 2018. "eCitizen and Other Popular Kenyan Websites are not Secure- Report". *Techweez*. https://techweez.com/2018/07/24/ecitizen-popular-kenyan-websites-not-secure-report/

76 Ibekwe N., 2015. "Over N121 billion wasted, Nigeria's troubled National ID Card project in fresh controversy". *Premium Times.* https://www.premiumtimesng.com/news/headlines/183720-over-n121-billion-wasted-nigerias-troubled-national-id-card-project-in-fresh-controversy.html

77 BBC News, 2017. "Malaysian data breach sees 46 million phone numbers leaked". *BBC*. https://www.bbc.com/news/technology-41816953

78 Babulal V., 2018. "Authorities probing data breach of 220,000 Malaysian organ donors". *New Straits Times.* https://www.nst.com.my/news/nation/2018/01/328253/authorities-probing-data-breach-220000-malaysian-organ-donors

79 Nyabola N., 2020.

80 Privacy International, 2019a.

81 Wasuna B., 2018. "How rogue IEBC staff minted cash from sale of voters' data". *The Star*. https://www.the-star.co.ke/news/2018-05-10-how-rogue-iebc-staff-minted-cash-from-sale-of-voters-data/

82 Muthuri R., Monyango F., and Karanja W., 2018. p 5.

83 Muthuri R., Monyango F., and Karanja W., 2018.

84 Chimhangwa K., 2020. "How Zimbabwe's biometric ID scheme (and China's AI aspirations) threw a wrench into the 2018 election". *GlobalVoices.* https://advox.globalvoices.org/2020/01/30/how-zimbabwes-biometric-id-scheme-and-chinas-ai-aspirations-threw-a-wrench-into-the-2018-election/

85 Hendrix S., 2020. "Benjamin Netanyahu's election app potentially exposed data for every Israeli voter". *The Washington Post.* https://www.washingtonpost.com/world/middle_east/benjamin-netanyahus-election-app-potentially-exposed-data-for-every-israeli-voter/2020/02/10/98f606c0-4bfe-11ea-967b-e074d302c7d4_story.html

86 Chi L., 2016. "Philippines elections hack 'leaks voter data". *BBC.* https://www.bbc.com/news/technology-36013713

87 Doshi V., 2018. "A security breach in India has left a billion people at risk of identity theft". *The Washington Post.* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/

88 Winder D., 2019. "A 'Government Database' Of 92 Million Citizen Records For Sale To Highest Bidder." *Forbes.* https://www.forbes.com/sites/daveywinder/2019/10/06/a-government-database-of-92-million-citizen-records-for-sale-to-highest-bidder/#47c572ea701b

89 van Zyl G., 2017. "Biggest ever SA data breach: 60 million ID numbers leaked on real estate server". *BizNews.* https://www.biznews.com/global-citizen/2017/10/20/biggest-ever-sa-data-breach

90 Gous N., 2017. "Top real estate company admits to being unwitting source of country's largest personal data breach". *Times Live.* https://www.timeslive.co.za/news/south-africa/2017-10-18-top-real-estate-company-admits-to-being-unwitting-source-of-countrys-largest-personal-data-breach/

91 Karabus J., 2019. "Charmin'. Garmin admits customers' full credit card data nicked from South African web store". *The Register.* https://www.theregister.co.uk/2019/09/13/garmin_breach_notification/

92 Tactical Tech, 2019. "Personal Data: Political Persuasion Inside the Influence Industry. How it works". T*actical Tech.* p. 30. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf

93 BusinessTech, 2018. "The average cost of a data breach in South Africa hits R36.5 million". *BusinessTech.* https://businesstech.co.za/news/it-services/257855/the-average-cost-of-a-data-breach-in-south-africa-hits-r36-5-million/

94 Mutung'u G., 2018. "The Influence Industry Data and Digital Election Campaigning in Kenya". *Tactical Technology Collective.* https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

95 Muthuri R., Monyango F., and Karanja W., 2018.

96 Privacy International, 2019b. "Africa: SIM Card Registration Only Increases Monitoring and Exclusion". *Privacy International.* https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion; Theodorou Y., Okong'o K., and Yongo E., 2019. Access to Mobile Services and Proof of Identity 2019. GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf

97 Privacy International, 2019b.

98 Privacy International, 2019b.

99 Idem

100 Kaye D., 2015. "Report on encryption, anonymity, and the human rights framework". United Nations Human Rights Council. p 18, paragraph 51. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

101 UK BBC Reality Check Team, 2019. "South Africa crime: Police figures show rising murder and sexual offences." https://www.bbc.com/news/world-africa-49673944

102 Crisis Group, 2015. "Al-Shabaab's Kenyan Ambitions." https://www.crisisgroup.org/africa/horn-africa/kenya/al-shabaab-s-kenyan-ambitions

103 BAKE, 2018. "State of the Internet in Kenya 2017". Bloggers Association of Kenya. https://www.ifree.co.ke/wp-content/uploads/2018/02/State-of-the-Internet-in-Kenya-report-2017.pdf

104 Paradigm International, 2018. "The Right to Privacy in Nigeria". *Privacy International.* Paragraph 40. https://www.privacyinternational.org/sites/default/files/2018-05/UPR_The%20Right%20to%20Privacy_Nigeria.pdf

105 Privacy International, 2019d. "Myanmar: Dangerous Plans for Biometric SIM Card Registration Must be Scrapped". *Privacy International.* https://privacyinternational.org/news-analysis/3303/myanmar-dangerous-plans-biometric-sim-card-registration-must-be-scrapped

106 Dahir A., 2020.

107 Dahir A. and Mureithi C., 2020. "Kenya's High Court Delays National Biometric ID Program". *The New York Times.* https://www.nytimes.com/2020/01/31/world/africa/kenya-biometric-ID-registry.html

108 Privacy International, 2019c. "Inside Niger's New Biometric Voting System". *Privacy International.* https://privacyinternational.org/long-read/3273/case-study-biometric-voting-cards

109 Latif A., 2020.

110 National Coalition of Human Rights Defenders of Kenya, 2019. "The Right to Privacy in Kenya". *Privacy International. Paragraph 54.* https://privacyinternational.org/sites/default/files/2019-12/The%20Right%20to%20Privacy%20in%20Kenya_35%20UPR%20session.pdf

111 Browne S., 2015. "Dark Matters: On the Surveillance of Blackness". *Duke University Press.*

112 Privacy International, 2020b. "The Hindsight Files 2020: Much More Than Politics". *Privacy International.* https://privacyinternational.org/news-analysis/3343/hindsight-files-2020-much-more-politics

113 Solomon S., 2018. "Cambridge Analytica Played Roles in Multiple African Elections ". *VOA News.* https://www.voanews.com/africa/cambridge-analytica-played-roles-multiple-african-elections

114 Halpern S., 2020.

115 Nyabola N., 2020.

116 Wasuna B., 2018. "How rogue IEBC staff minted cash from sale of voters' data". The Star. https://www.the-star.co.ke/news/2018-05-10-how-rogue-iebc-staff-minted-cash-from-sale-of-voters-data/

117 Roberts T., 2019. "Transcript: Digital Democracy, Analogue Politics – Interview with Nanjala Nyabola". IDS. https://www.ids.ac.uk/wp-content/uploads/2019/06/9.-Nanjala-Nyabola-transcript.pdf

118 Coppins M., 2020.

119 Computational Propaganda Project, 2019. "Coverage: 2019 Global Inventory of Social Media Manipulation". *Oxford Internet Institute.* https://comprop.oii.ox.ac.uk/press/in-the-news/coverage-2019-cybertroops/

120 Poonam S. and Bansal S., 2019. "Misinformation Is Endangering India's Election". *The Atlantic.* https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/

121 Iwanek K., 2018. "WhatsApp, Fake News? The Internet and Risks of Misinformation in India." *The Diplomat.* https://thediplomat.com/2018/07/whatsapp-fake-news-the-internet-and-risks-of-misinformation-in-india/

122 Human Rights Watch, 2018.

123 Privacy International, 2018.

124 Muthuri R., Monyango F., and Karanja W., 2018.

125 Nyabola N., 2020.

126 Moore J., 2018.

127 Privacy International, 2017b. "Voter Profiling in the 2017 Kenyan Election". *Privacy International.* https://privacyinternational.org/blog/845/voter-profiling-2017-kenyan-election

128 Okeyo A., 2018. "From African American Voters to African Nations, Cambridge Analytica Wages 'Cultural Warfare". *The Progressive.* https://progressive.org/dispatches/from-african-american-voters-to-african-nations-cambridge-analytica-180521/

129 Bright S., 2017.

130 York G., 2018. "Cambridge Analytica parent company manipulated Nigeria's 2007 election, documents show". *The Globe and Mail*. https://www.theglobeandmail.com/world/article-cambridge-analytica-parent-company-manipulated-nigerias-2007-election/

131 UK Parliament Select Committee on Culture, Media, and Sport, 2018. "Disinformation and 'fake news': Interim Report". *UK Parliament.* https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36309.htm

132 Cadwalladr C., 2018. "Revealed: graphic video used by Cambridge Analytica to influence Nigerian election". *T he Guardian.* https://www.theguardian.com/uk-news/2018/apr/04/cambridge-analytica-used-violent-video-to-try-to-influence-nigerian-election

133 Obulutsa G., 2017. " Kenya president's election campaign used firm hired by Trump: privacy group". *Reuters.* https://www.reuters.com/article/us-kenya-politics/kenya-presidents-election-campaign-used-firm-hired-by-trump-privacy-group-idUSKBN1E82QS

134 Cadwalladr C., 2018.

135 Rodny-Gumede Y., 2017. "Fake news: the internet has turned an age-old problem into a new threat". *The Conversation.* http://theconversation.com/fake-news-the-internet-has-turned-an-age-old-problem-into-a-new-threat-72111

136 Segal D., 2018.

137 Mutung'u G., 2018.

138 Ibekwe N., 2015. "Over N121 billion wasted, Nigeria's troubled National ID Card project in fresh controversy". *Premium Times.* https://www.premiumtimesng.com/news/headlines/183720-over-n121-billion-wasted-nigerias-troubled-national-id-card-project-in-fresh-controversy.html

139 Muthuri R., Monyango F., and Karanja W., 2018.

140 Mutung'u G., 2018. p. 14.

141 Coppins M., 2020.

142 Hezron N., 2008. "From Cyberspace to the Public: Rumor, Gossip and Hearsay in the Paradoxes of the 2007 General Election in Kenya". *12th General Assembly Governing the African Public Sphere.* https://www.codesria.org/IMG/pdf/Hezron_Ndunde.pdf

143 Idem.

144 Idem.

145 Goldman A., Barnes J., Haberman M., and Fandos N., 2020. "Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump". *The New York Times.* https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html

146 National Coalition of Human Rights Defenders of Kenya, 2019.; Paradigm International, 2018.

147 Posetti J., Simon F., and Shabbir N. "Reporting elections on the frontline of the disinformation war". *Reuters Institute.* https://reutersinstitute.politics.ox.ac.uk/risj-review/reporting-elections-frontline-disinformation-war

148 Nyabola N., 2020.

149 Mozur P. and Krolik A., 2019. "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers ". *The New York Times.* https://www.nytimes.com/2019/12/17/technology/china-surveillance.html

150 Campbell C., 2019. "How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens". *Time.* https://time.com/collection/davos-2019/5502592/china-social-credit-score/

151 O'Brien D., 2019. "Massive Database Leak Gives Us a Window into China's Digital Surveillance State". *EFF.* https://www.eff.org/fr/deeplinks/2019/03/massive-database-leak-gives-us-window-chinas-digital-surveillance-state

152 Mozur P., 2019. "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority". *The New York Times.* https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

153 International-mobile-subscriber-identity (IMSI) catchers are telephone eavesdropping devices used for intercepting mobile phone traffic and tracking location data of mobile phone users.

154 Mozur P. and Krolik A., 2019.

155 Freedom House, 2020. "China" *Freedom House.* https://freedomhouse.org/country/china/freedom-world/2020

156 Shi-Kupfer K. and Ohlberg M., 2019. "China Digital Rise". *Mercator Institute for China Studies.* https://www.merics.org/sites/default/files/2019-04/MPOC_No.7_ChinasDigitalRise_web_4.pdf

157 Human Rights Watch, 2019. "How Mass Surveillance Works in Xinjiang, China". *The Human Rights Watch.* https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang

158 Weinberger S., 2019. "Private Surveillance Is a Lethal Weapon Anybody Can Buy ". *The New York Times.* https://www.nytimes.com/2019/07/19/opinion/private-surveillance-industry.html

159 Human Rights Council, 2019. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". UN General Assembly. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement

160 KeepItOn, 2018. "The State of Internet Shutdowns Around the World". KeepItOn. https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf

161 Deloitte, 2016. "The economic impact of disruptions to Internet connectivity". Deloitte. https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf

162 Chutel L., 2019. "Zimbabwe's government shut down the internet after fuel price protests turned deadly". *Quartz Africa.* https://qz.com/africa/1524405/zimbabwe-protest-internet-shut-down-military-deployed-5-dead/

163 UN Human Rights Council, 2019. "Surveillance and human rights". *United Nations Digital Library.* https://digitallibrary.un.org/record/3814512?ln=en

164 CIPIT, 2017. "Safaricom and Internet Traffic Tampering". CIPIT. https://blog.cipit.org/wp-content/uploads/2017/03/Final-March-Brief-pages.pdf

165 Privacy International, 2017.

166 National Coalition of Human Rights Defenders of Kenya, 2019. p. 9.

167 Freedom House, 2019.

168 Freedom House, 2019b. "Freedom in the World 2019- Nigeria". Freedom House. https://freedomhouse.org/country/nigeria/freedom-world/2019

169 Ekwealor V., 2019. "Nigeria's president refused to sign its digital rights bill, what happens now?". Techpoint Africa. https://techpoint.africa/2019/03/27/nigerian-president-declines-digital-rights-bill-assent/

170 Freedom House, 2019b.

171 Poetranto I., 2013. "Paradigm Initiative Nigeria Seeks Information on Surveillance Systems in Nigeria". *The Citizen Lab, University of Toronto.* https://citizenlab.ca/2013/10/the-cyber-stewards-network-speak-out-on-prism/

172 Paradigm International, 2018.

173 Burt C., 2020. "New approaches to identity altering government operations to take the spotlight at ID4Africa 2020". BiometricUpdate. https://www.biometricupdate.com/202003/new-approaches-to-identity-altering-government-operations-to-take-the-spotlight-at-id4africa-2020

174 Dahir A., 2020.; Dahir A. and Mureithi C., 2020.; England R., "Kenya halts biometric ID scheme over discrimination fears". *Engadget.* https://www.engadget.com/2020-02-03-kenya-halts-biometric-id-scheme-discrimination-fears.html

175 Madianou M., 2019

176 Dahir A. and Mureithi C., 2020.

177 Idem

178 Idem

179 IDEA, 2017. "ICTs in Elections Database- Voter registration and identification". *Institute for Democracy and Electoral Assistance.* https://www.idea.int/data-tools/question-countries-view/738/Africa/cnt

180 Harris M., 2019. "An Eye-Scanning Lie Detector Is Forging a Dystopian Future," *Wired.* https://www.wired.com/story/eye-scanning-lie-detector-polygraph-forging-a-dystopian-future/ ; Katwala A., 2019. "The Race to Create a Perfect Lie Detector – and the Dangers of Succeeding," *The Guardian.* https://www.theguardian.com/technology/2019/sep/05/the-race-to-create-a-perfect-lie-detector-and-the-dangers-of-succeeding

181 Oxygen Forensics, 2019. "Detective 11.5". Oxygen Forensics. https://www.oxygen-forensic.com/uploads/press_kit/OF_RN_11_5_web.pdf

182 Kwet M., 2019.

183 Telford T., 2019. "'Emotion detection' AI is a $20 billion industry. New research says it can't do what it claims." *The Washington Post.* https://www.washingtonpost.com/business/2019/07/31/emotion-detection-ai-is-billion-industry-new-research-says-it-cant-do-what-it-claims/

184 Halpern S., 2020.

185 Barrett L., Adochs R., and Marsella S., 2019. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements". *Psychological Science in the Public Interest.* https://journals.sagepub.com/eprint/SAUES8UM69EN8TSMUGF9/full; Lohr S., 2018. "Facial Recognition Is Accurate If You're A White Guy". *The New York Times.* https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html; and Singer N, 2019. "Amazon Is Pushing Facial Technology That a Study Says Could Be Biased". *The New York Times.* https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html

186 Pauwels E., 2019. "The New Geopolitics of Converging Risks". United Nations University. https://collections.unu.edu/eserv/UNU:7308/PauwelsAIGeopolitics.pdf

187 Idem

188 Galston W., 2020. "Is seeing still believing?". *Brookings Institute.* https://www.brookings.edu/research/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/

189 Stupp C., 2019. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case". *The Wall Street Journal.* https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

190 Lomas N. 2017. "Lyrebird is a voice mimic for the fake news era." TechCrunch. https://techcrunch.com/2017/04/25/lyrebird-isa-voice-mimic-for-the-fake-news-era/

191 Cole S., 2019. "This Program Makes It Even Easier to Make Deepfakes". *Vice News.* https://www.vice.com/en_us/article/kz4amx/fsgan-program-makes-it-even-easier-to-make-deepfakes; ODSC - Open Data Science, 2019. "FSGAN: Subject Agnostic Face Swapping and Reenactment," *Medium.* https://medium.com/@ODSC/fsgan-subject-agnostic-face-swapping-and-reenactment-2f033b0ea83c

192 Nirkin Y., Keller Y., and Hassner T., 2019. "FSGAN: Subject Agnostic Face Swapping and Reenactment" *arXiv.* https://arxiv.org/pdf/1908.05932.pdf

193 Faife C., 2019. "In Africa, Fear of State Violence Informs Deepfake Threat". *Witness.* https://blog.witness.org/2019/12/africa-fear-state-violence-informs-deepfake-threat/

194 Human Rights Council, 2018. "The right to privacy in the digital age". UN General Assembly. https://undocs.org/A/HRC/39/29

195 Human Rights Council, 2018. "The right to privacy in the digital age". UN General Assembly. https://undocs.org/A/HRC/39/29

196 AI Now Institute, 2019.

197 Chutel L., 2018. "China is exporting facial recognition software to Africa, expanding its vast database". *Quartz Africa.* https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

198 Woodhams S., 2019. "How China Exports Repression to Africa". *The Diplomat.* https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/

199 Hawkins A., 2018. "Beijing's Big Brother Tech Needs African Faces" *Foreign Policy.* https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/

200 Kwet M., 2019.

201 Kwet M., 2019.

202 Idem

203 Privacy International, 2020b.

204 SecurityToday, 2018. "Biometrics Market to Hit $50 Billion by 2024". *SecurityToday.* https://securitytoday.com/articles/2018/02/08/biometrics-market-to-hit-50-billion-by-2024.aspx?admgarea=ht.emergingtechnologies&m=1

205 Dahir A., 2020.

206 Dermalog, 2014. "Nigeria: DERMALOG wins 50 million dollar contract". *Dermalog.* https://www.dermalog.com/news/article/dermalog-wins-50-million-dollar-contract/

207 Lee J., 2017. " Laxton Group to supply biometric voter registration kits for Zimbabwe elections". *BiometricUpdate*. https://www.biometricupdate.com/201706/laxton-group-to-supply-biometric-voter-registration-kits-for-zimbabwe-elections

208 Feldstein S., 2019. "The Global Expansion of AI Surveillance". *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

209 Masood E., How China is Redrawing the Map of World Science, Nature, May 1, 2019. https://www.nature.com/immersive/d41586-019-01124-7/index.htm

210 Link J., 2019. "How Huawei could survive Trump". *The Washington Post.* https://www.washingtonpost.com/politics/2019/06/10/what-do-we-know-about-huaweis-africa-presence/

211 Parkinson J., Bariyo N., and Chin J., 2019.

212 Chutel L., 2018.; Hawkins M., 2019.

213 He L., 2019. "Africa's top smartphone maker soars 64% in debut on China's tech market". *CNN*. *https://www.cnn.com/2019/09/30/tech/transsion-holdings-africa-ipo/index.html*

214 UN Human Rights Office, 2019b. "The 2019 report on the surveillance industry ". United Nations. https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx

215 Chimbelu C., 2019. "Investing in Africa's tech infrastructure. Has China won already?". *DW.* https://www.dw.com/en/investing-in-africas-tech-infrastructure-has-china-won-already/a-48540426

216 Shahbaz A. 2018. "The Rise of Digital Authoritarianism". *Freedom House.* https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism

217 Republic of Kenya, 2018. "The Computer Misuse and Cybercrimes Act, 2018". http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

218 Freedom House. "Kenya". https://freedomhouse.org/country/kenya

219 Ibid.

220 Khamadi S., 2017. " Paul Odhiambo arrested for 'publishing inflammatory messages' on Facebook". *iFree.* https://www.ifree.co.ke/2017/07/paul-odhiambo-arrested-publishing-inflammatory-messages-facebook/

221 Ojekunle A., 2019. "President Buhari has rejected a bill seeking to protect the rights of internet users in Nigeria from infringement". *Pulse.* https://www.pulse.ng/bi/politics/buhari-rejects-digital-rights-bill-a-bill-seeking-to-protect-the-rights-of-internet/zztwxz1

222 Freedom House, 2019b.

223 Republic of Nigeria, 2015. "Cybercrimes Bill". https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

224 Paradigm International, 2018.

225 Page J., O'Keeffe K., Taylor R., 2019. " America's Undersea Battle With China for Control of the Global Internet Grid". *The Wall Street Journal.* https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466

226 Privacy International, 2020.

227 Shahbaz A., 2018. " The Rise of Digital Authoritarianism". Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

228 Masood E., 2019. " How China is redrawing the map of world science". *Nature.* https://www.nature.com/immersive/d41586-019-01124-7/index.html

229 Albert E., 2017. "China in Africa". *Council on Foreign Relations.* https://www.cfr.org/backgrounder/china-africa

230 Masood E., 2019.

231 Roussi A., 2019. " Chinese investments fuel growth in African science". *Nature.* https://www.nature.com/immersive/d41586-019-01398-x/index.html

232 Dahir, A., 2018. "Kenya's M-Pesa mobile money service now works with China's WeChat Pay". *Quartz Africa*. https://qz.com/africa/1482013/safaricoms-m-pesa-connects-with-chinas-wechat-pay/

233 Pauwels E., 2018. "China is pushing hard to overtake Silicon Valley and win the biotech race, and gain control of the world's biological data". *South China Morning Post.* https://www.scmp.com/comment/insight-opinion/united-states/article/2174533/china-pushing-hard-overtake-silicon-valley-and

234 Shen Q., 2019. "China Will Likely Corner the 5G Market—and the US Has No Plan". *Wired*. https://www.wired.com/story/china-will-likely-corner-5g-market-us-no-plan/

235 Roussi A., 2019.

236 Ibukun Y., 2018. "China Exim Bank Loans $328 Million for Nigerian Internet Project". *Bloomberg*. https://www.bloomberg.com/news/articles/2018-09-01/china-exim-bank-loans-328-million-for-nigerian-internet-project

237 Chou R., 2020. "South Africa's Rain and Huawei Build the First 5G Transport Networks Using OXC+200G Solution". *Bloomberg*. https://www.bloomberg.com/press-releases/2020-02-27/south-africa-s-rain-and-huawei-build-the-first-5g-transport-networks-using-oxc-200g-solution

238 Miriri D., 2020. "Kenya's Safaricom to consider Huawei as supplier for 5G network". *Reuters*. https://www.reuters.com/article/us-kenya-safaricom/kenyas-safaricom-to-consider-huawei-as-supplier-for-5g-network-idUSKBN20E1RG

239 Huawei. "Huawei Empowers Japan's CyberAgent to Build an IDN-Capable Cloud Data Center Network with All-Fixed Switches." https://e.huawei.com/topic/leading-new-ict-en/cyberagent-case.html

240 El Kadi T., 2019. "The Promise and Peril of the Digital Silk Road". *Chatham House*. https://www.chathamhouse.org/expert/comment/promise-and-peril-digital-silk-road

241 Munshi N., 2020. "Africa's cloud computing boom created data centre gold rush". *Financial Times*. https://www.ft.com/content/402a18c8-5a32-11ea-abe5-8e03987b7b20

242 Prasso S., 2019. "China' Silk Road is Looking More Like an Iron Curtain", *Bloomberg*. https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain

243 Parkinson J., Bariyo N., and Chin J., 2019

244 Link J., 2019.

245 Moss S., 2019. "Huawei to build Konza data center and smart city in Kenya, with Chinese concessional loan". *Data Center Dynamics*. https://www.datacenterdynamics.com/en/news/huawei-build-konza-data-center-and-smart-city-kenya-chinese-concessional-loan/

246 Parkinson J., Bariyo N., and Chin J., 2019. "Huawei Technicians Helped African Governments Spy on Political Opponents". *The Wall Street Journal*. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

247 Parkinson J., Bariyo N., and Chin J., 2019

248 Parkinson J., Bariyo N., and Chin J., 2019

249 Alba D., and Frenkel S., 2019. "Russia Tests New Disinformation Tactics in Africa to Expand Influence". *The New York Times*. https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html; Harding L. and Burke J., 2019. "Leaked documents reveal Russian effort to exert influence in Africa". *The Guardian*. https://www.theguardian.com/world/2019/jun/11/leaked-documents-reveal-russian-effort-to-exert-influence-in-africa

250 Schwirtz M. and Borgia G., 2019.

251 Harding L. and Burke J., 2019.

252 Isaac M., 2019. "Facebook Finds New Disinformation Campaigns and Braces for 2020 Torrent". *The New York Times*. https://www.nytimes.com/2019/10/21/technology/facebook-disinformation-russia-iran.html

253 Ward C., Polglase K., Shukla S., Mezzofiore G., and Lister T., 2020.

254 Rankin J., 2020. "Russian media 'spreading Covid-19 disinformation". *The Guardian*. https://www.theguardian.com/world/2020/mar/18/russian-media-spreading-covid-19-disinformation

255 Bradsher K. and Behnhold K., 2019. "World Leaders at Davos Call for Global Rules on Tech". *The New York Times*. https://www.nytimes.com/2019/01/23/technology/world-economic-forum-data-controls.html

256 Gross A., Murgia M., and Yang Y., 2019.

257 United Nations General Assembly, 2019. "General Assembly Approves $3.07 Billion Programme Budget as It Adopts 22 Resolutions, 1 Decision to Conclude Main Part of Seventy-Fourth Session". https://www.un.org/press/en/2019/ga12235.doc.htm

258 Source: Map based on 2019 Vote on Countering the Use of Information and Communication Technologies for Criminal Purposes

259 Human Rights Council, 2019b. "Report on the rights to freedom of peaceful assembly and of association: The Digital Age". UN General Assembly. https://www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/DigitalAge.aspx

260 Schulze E., 2019. "Russia just brought in a law to try to disconnect its internet from the rest of the world". *CNBC*. https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html

261 Fielder M., 2015. "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity". *Council on Foreign Relations.* https://www.cfr.org/blog/african-union-cybersecurity-convention-missed-human-rights-opportunity

262 Dahir A., 2019b. "The African Union is doubling down on deepening its relationship with Huawei". *Quartz Africa*. https://qz.com/africa/1632111/huawei-african-union-sign-deal-to-boost-5g-ai-cloud-computing/

263 UN Human Rights Office, 2019. "Cooperation Agreement". https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25010&LangID=E

264 Pauwels E., 2019.

265 Ben-Hassine W., 2018. "Government Policy for the Internet Must Be Rights-Based and User-Centered". *UN Chronicle.* https://unchronicle.un.org/article/government-policy-internet-must-be-rights-based-and-user-centred

266 Privacy International, 2020a

267 Dahir A., 2020.

268 Privacy International, 2020c. "Analysis of Kenya's Data Protection Act, 2019". *Privacy International*. https://privacyinternational.org/advocacy/3348/analysis-kenyas-data-protection-act-2019

269 NITDA, 2019. "Nigeria Data Protection Regulation". https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf

270 Martin-Rozumilowicz B. and Kuzel R., 2019. "Social Media, Disinformation and Electoral Integrity". *International Foundation for Electoral Systems.* https://www.ifes.org/sites/default/files/ifes_working_paper_social_media_disinformation_and_electoral_integrity_august_2019_0.pdf

271 Idem, p. 26.

272 AfricaTimes, 2019. " Facebook expands fact-checking to 15 African nations". *AfricaTimes.* https://africatimes.com/2019/10/10/facebook-expands-fact-checking-to-15-african-nations/

273 Kramer F., 2019. "Fact-checking in Africa". *Konrad-Adenauer-Stiftung.* https://www.kas.de/en/web/medien-afrika/veranstaltungsberichte/detail/-/content/fact-checking-in-africa

274 Kornbluh K., Goodman E., and Weiner E., 2020. "Safeguarding Democracy Against Disinformation". *German Marshall Fund of the United States.* http://www.gmfus.org/publications/safeguarding-democracy-against-disinformation?utm_source=email&utm_medium=email&utm_campaign=ww%202020-03-25

275 Tonisi L., 2019. "Fake news monitor launched for 2019 election season". *Daily Maverick.* https://www.dailymaverick.co.za/article/2019-04-02-fake-news-monitor-launched-for-2019-election-season/

276 Roberts T., 2019. "Transcript: Digital Democracy, Analogue Politics – Interview with Nanjala Nyabola". IDS. https://www.ids.ac.uk/wp-content/uploads/2019/06/9.-Nanjala-Nyabola-transcript.pdf

# Bibliography and Selected List of Expert Interviews and Consultation

**Consultation** with experts from the UN Department of Political and Peacebuilding Affairs (UN DPPA) & the Social Sciences Research Council (SSRC), 30 January 2020

- Susan Benesch, Dangerous Speech Project, Berkman Klein Center for Internet & Society, Harvard University
- Idayat Hassan, Center for Democracy and Development, Nigeria
- Mona Kleinberg, University of Massachusetts – Lowell
- Thong Nguyen, International Peace Institute
- Nanjala Nyabola, Independent Research, Kenya
- Duncan Omanga, African Peacebuilding Network and Next Generation Social Sciences in Africa, SSRC
- Jonathan Corpus Ong, University of Massachusetts, Amherst
- Jason Rhody, Digital Culture, Social Data Initiative, Media and Democracy, SSRC
- Sahana Udupa, Ludwig Maximilian University, Munich
- Cody Buntain, New Jersey Institute of Technology
- Endalkachew Chala, Hamline University

## Expert Interviews

- Karen Allen, Senior Research Advisor, Emerging Threats in Africa, Institute for Security Studies, Pretoria, February 2, 2020
- Caio Machado, Oxford Internet Institute and University of Sao Paulo, December 18, 2019
- Diego Aranha, Cybersecurity Exert – Electronic Voting in Brazil, Department of Engineering, University Aarhus and University of Campinas, December 20, 2019
- Christina Nemr, Cybersecurity and Disinformation Expert, US Department of State and Park Advisors, December 20, 2019
- Rushdi Nackerdien, Regional Director: Africa, IFES, December 13, 2019
- Niels Nagelhus Schia, Senior Research Fellow, NUPI (Norwegian Institute of International Affairs), Center for Cybersecurity Studies, December 13, 2019
- Paul Sambo, Expert on Election in South Africa, University of Pretoria, December 11, 2019
- Steve Martin, UN Electoral Assistance Division, December 9, 2019
- Maarten Halff, UN Electoral Assistance Division, December 9, 2019
- Professor Jarno Limnell, Cybersecurity, University of Aalto (Finland) and CEO of Tosibox, December 9, 2019

# Bibliography


AfricaTimes, 2019. "Facebook expands fact-checking to 15 African nations". *AfricaTimes*. https://africatimes.com/2019/10/10/facebook-expands-fact-checking-to-15-african-nations/

AI Now Institute, 2019. "AI Now 2019 Report". https://ainowinstitute.org/AI_Now_2019_Report.html

Alba D., and Frenkel S., 2019. "Russia Tests New Disinformation Tactics in Africa to Expand Influence". *The New York Times*. https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html

Albert E., 2017. "China in Africa". *Council on Foreign Relations*. https://www.cfr.org/backgrounder/china-africa

Babulal V., 2018. "Authorities probing data breach of 220,000 Malaysian organ donors". *New Straits Times*. https://www.nst.com.my/news/nation/2018/01/328253/authorities-probing-data-breach-220000-malaysian-organ-donors

Bailey N., 2017. "East African States Adopt China's Playbook on Internet Censorship". *Freedom House*. https://freedomhouse.org/article/east-african-states-adopt-chinas-playbook-internet-censorship

BAKE, 2018. "State of the Internet in Kenya 2017". Bloggers Association of Kenya. https://www.ifree.co.ke/wp-content/uploads/2018/02/State-of-the-Internet-in-Kenya-report-2017.pdf

Barrett L., Adochs R., and Marsella S., 2019. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements". *Psychological Science in the Public Interest*. https://journals.sagepub.com/eprint/SAUES8UM69EN8TSMUGF9/full

BBC News, 2017. "Malaysian data breach sees 46 million phone numbers leaked". *BBC*. https://www.bbc.com/news/technology-41816953

Ben-Hassine W., 2018. "Government Policy for the Internet Must Be Rights-Based and User-Centred". *UN Chronicle*. https://unchronicle.un.org/article/government-policy-internet-must-be-rights-based-and-user-centred

Bitzonis T., 2020. "Ghanaian Think-tank IMANI Denounces Government Effort to Acquire New Biometric Voter Registration System". *FindBiometrics*. https://findbiometrics.com/biometrics-news-ghanaian-think-tank-imani-against-ec-over-new-biometric-voter-registration-system-031103/

Bradsher K. and Behnhold K., 2019. "World Leaders at Davos Call for Global Rules on Tech". *The New York Times*. https://www.nytimes.com/2019/01/23/technology/world-economic-forum-data-controls.html

BPU Holdings, 2018. "ZimGo Polling Is First Emotion AI Election Analytics and Forecasting Service for US Campaigns". *BusinessWire*. https://www.businesswire.com/news/home/20180430005331/en/ZimGo-Polling-Emotion-AI-Election-Analytics-Forecasting

Bright S., 2017. "After Trump, "big data" firm Cambridge Analytica is now working in Kenya." *BBC*. https://www.bbc.com/news/blogs-trending-40792078

Burt C., 2020. "New approaches to identity altering government operations to take the spotlight at ID4Africa 2020". *BiometricUpdate*. https://www.biometricupdate.com/202003/new-approaches-to-identity-altering-government-operations- zto-take-the-spotlight-at-id4africa-2020

BusinessTech, 2018. "The average cost of a data breach in South Africa hits R36.5 million". *BusinessTech*. https://businesstech.co.za/news/it-services/257855/the-average-cost-of-a-data-breach-in-south-africa-hits-r36-5-million/

Cadwalladr C., 2018. "Revealed: graphic video used by Cambridge Analytica to influence Nigerian election". *The Guardian*. https://www.theguardian.com/uk-news/2018/apr/04/cambridge-analytica-used-violent-video-to-try-to-influence-nigerian-election

Cadwalladr C., 2019. "Cambridge Analytica a year on: 'a lesson in institutional failure". *The Guardian*. https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie

Cadwalladr C., 2020. “Fresh Cambridge Analytica leak ‘shows global manipulation is out of control”. *The Guardian*. https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation

Calistra C., 2015. “Emotion Analysis in the Real World”. *Kairos*. https://www.kairos.com/blog/emotion-analysis-in-the-real-world

Campbell C., 2019. “How China Is Using “Social Credit Scores” to Reward and Punish Its Citizens”. *Time*. https://time.com/collection/davos-2019/5502592/china-social-credit-score/

Chi L., 2016. “Philippines elections hack 'leaks voter data”. *BBC*. https://www.bbc.com/news/technology-36013713

Chimbelu C., 2019. “Investing in Africa's tech infrastructure. Has China won already?”. *DW*. https://www.dw.com/en/investing-in-africas-tech-infrastructure-has-china-won-already/a-48540426

Chimhangwa K., 2020. “How Zimbabwe's biometric ID scheme (and China’s AI aspirations) threw a wrench into the 2018 election”. *GlobalVoices*. https://advox.globalvoices.org/2020/01/30/how-zimbabwes-biometric-id-scheme-and-chinas-ai-aspirations-threw-a-wrench-into-the-2018-election/

Chou R., 2020. “South Africa's Rain and Huawei Build the First 5G Transport Networks Using OXC+200G Solution”. *Bloomberg*. https://www.bloomberg.com/press-releases/2020-02-27/south-africa-s-rain-and-huawei-build-the-first-5g-transport-networks-using-oxc-200g-solution

Chutel L., 2018. “China is exporting facial recognition software to Africa, expanding its vast database”. *Quartz Africa.* https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

Chutel L., 2019. “Zimbabwe’s government shut down the internet after fuel price protests turned deadly“. *Quartz Africa.* https://qz.com/africa/1524405/zimbabwe-protest-internet-shut-down-military-deployed-5-dead/

CIPIT, 2017. “Safaricom and Internet Traffic Tampering”. CIPIT. https://blog.cipit.org/wp-content/uploads/2017/03/Final-March-Brief-pages.pdf

Cole S., 2019. “This Program Makes It Even Easier to Make Deepfakes”. *Vice News.* https://www.vice.com/en_us/article/kz4amx/fsgan-program-makes-it-even-easier-to-make-deepfakes

Commission of Inquiry into Post-Election Violence (CIPEV), 2018. “Final Report”. https://reliefweb.int/sites/reliefweb.int/files/resources/15A00F569813F4D549257607001F459D-Full_Report.pdf

Computational Propaganda Project, 2019. “Coverage: 2019 Global Inventory of Social Media Manipulation”. *Oxford Internet Institute.* https://comprop.oii.ox.ac.uk/press/in-the-news/coverage-2019-cybertroops/

Coppins M, 2020. “The Billion-Dollar Disinformation Campaign to Reelect the President”. *The Atlantic.* https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/

Crawford K., 2019. “Regulate facial-recognition Technology”. *Nature.* https://media.nature.com/original/magazine-assets/d41586-019-02514-7/d41586-019-02514-7.pdf

Dahir A., 2017. “WhatsApp and Facebook are driving Kenya’s fake news cycle”. *Quartz Africa.* https://qz.com/africa/1033181/whatsapp-and-facebook-are-driving-kenyas-fake-news-cycle-ahead-of-august-elections/

Dahir, A., 2018. “Kenya’s M-Pesa mobile money service now works with China’s WeChat Pay”. *Quartz Africa.* https://qz.com/africa/1482013/safaricoms-m-pesa-connects-with-chinas-wechat-pay/

Dahir A., 2019. “Chinese firms are driving the rise of AI surveillance across Africa”. *Quartz Africa.* https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa/

Dahir A., 2019b. “The African Union is doubling down on deepening its relationship with Huawei”. *Quartz Africa.* https://qz.com/africa/1632111/huawei-african-union-sign-deal-to-boost-5g-ai-cloud-computing/

Dahir A., 2020. “Kenya’s New Digital IDs May Exclude Millions of Minorities”. *The New York Times.* https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html

Dahir A. and Mureithi C., 2020. “Kenya’s High Court Delays National Biometric ID Program”. *The New York Times.* https://www.nytimes.com/2020/01/31/world/africa/kenya-biometric-ID-registry.html

Deloitte, 2016. “The economic impact of disruptions to Internet connectivity”. Deloitte. https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf

Dermalog, 2014. “Nigeria: DERMALOG wins 50 million dollar contract”. Dermalog. https://www.dermalog.com/news/article/dermalog-wins-50-million-dollar-contract/

Doshi V., 2018. "A security breach in India has left a billion people at risk of identity theft". *The Washington Post.* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/

Ekwealor V., 2019. "Nigeria's president refused to sign its digital rights bill, what happens now?". *Techpoint Africa.* https://techpoint.africa/2019/03/27/nigerian-president-declines-digital-rights-bill-assent/

El Kadi T., 2019. "The Promise and Peril of the Digital Silk Road". *Chatham House.* https://www.chathamhouse.org/expert/comment/promise-and-peril-digital-silk-road

England R., "Kenya halts biometric ID scheme over discrimination fears". *Engadget.* https://www.engadget.com/2020-02-03-kenya-halts-biometric-id-scheme-discrimination-fears.html

Etter L., 2017. "What Happens When the Government Uses Facebook as a Weapon?" *Bloomberg Businessweek.* https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook

Faife C., 2019. "In Africa, Fear of State Violence Informs Deepfake Threat". *Witness.* https://blog.witness.org/2019/12/africa-fear-state-violence-informs-deepfake-threat/

Fielder M., 2015. "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity". *Council on Foreign Relations.* https://www.cfr.org/blog/african-union-cybersecurity-convention-missed-human-rights-opportunity

Freedom House. "Kenya". https://freedomhouse.org/country/kenya

Feldstein S., 2019. "The Global Expansion of AI Surveillance". *Carnegie Endowment for International Peace.* https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Freedom House, 2019. "Freedom on the Net 2019- Kenya". *Freedom House.* https://freedomhouse.org/country/kenya/freedom-net/2019

Freedom House, 2019b. "Freedom in the World 2019- Nigeria". *Freedom House.* https://freedomhouse.org/country/nigeria/freedom-world/2019

Freedom House, 2020. "China" *Freedom House.* https://freedomhouse.org/country/china/freedom-world/2020

Galston W., 2020. "Is seeing still believing?". *Brookings Institute.* https://www.brookings.edu/research/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/

Goel V., 2018. "India's Top Court Limits Sweep of Biometric ID Program". *The New York Times.* https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html

Goel V. and Rahman, SA., 2019. "When Rohingya Refugees Fled to India, Hate on Facebook Followed ". *The New York Times.* https://www.nytimes.com/2019/06/14/technology/facebook-hate-speech-rohingya-india.html

Goldman A., Barnes J., Haberman M., and Fandos N., 2020. "Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump". *The New York Times.* https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html

Gous N., 2017. "Top real estate company admits to being unwitting source of country's largest personal data breach". *Times Live.* https://www.timeslive.co.za/news/south-africa/2017-10-18-top-real-estate-company-admits-to-being-unwitting-source-of-countrys-largest-personal-data-breach/

Gross A., Murgia M., and Yang Y., 2019. "Chinese tech groups shaping UN facial recognition standards". *Financial Times.* https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67

Halpern S., 2020. "The Neuroscience of Picking a Presidential Candidate. *The New Yorker.* https://www.newyorker.com/tech/annals-of-technology/the-neuroscience-of-picking-a-presidential-candidate

Harding L. and Burke J., 2019. "Leaked documents reveal Russian effort to exert influence in Africa". *The Guardian.* https://www.theguardian.com/world/2019/jun/11/leaked-documents-reveal-russian-effort-to-exert-influence-in-africa

Harris M., 2019. "An Eye-Scanning Lie Detector Is Forging a Dystopian Future," *Wired.* https://www.wired.com/story/eye-scanning-lie-detector-polygraph-forging-a-dystopian-future/

Hawkins A., 2018. "Beijing's Big Brother Tech Needs African Faces" *Foreign Policy.* https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/

HaystaqDNA. https://haystaqdna.com/

He L., 2019. "Africa's top smartphone maker soars 64% in debut on China's tech market". *CNN*. https://www.cnn.com/2019/09/30/tech/transsion-holdings-africa-ipo/index.html

Hendrix S., 2020. "Benjamin Netanyahu's election app potentially exposed data for every Israeli voter". *The Washington Post.* https://www.washingtonpost.com/world/middle_east/benjamin-netanyahus-election-app-potentially-exposed-data-for-every-israeli-voter/2020/02/10/98f606c0-4bfe-11ea-967b-e074d302c7d4_story.html

Hezron N., 2008. "From Cyberspace to the Public: Rumor, Gossip and Hearsay in the Paradoxes of the 2007 General Election in Kenya". *12th General Assembly Governing the African Public Sphere.* https://www.codesria.org/IMG/pdf/Hezron_Ndunde.pdf

Huawei. "Huawei Empowers Japan's CyberAgent to Build an IDN-Capable Cloud Data Center Network with All-Fixed Switches." https://e.huawei.com/topic/leading-new-ict-en/cyberagent-case.html

Human Rights Council, 2018. "The right to privacy in the digital age". UN General Assembly. https://undocs.org/A/HRC/39/29

Human Rights Council, 2019. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". UN General Assembly. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement

Human Rights Council, 2019b. "Report on the rights to freedom of peaceful assembly and of association: The Digital Age". UN General Assembly. https://www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/DigitalAge.aspx

Human Rights Watch, 2018. "Kenya- Events of 2017". *HRW*. https://www.hrw.org/world-report/2018/country-chapters/kenya

Human Rights Watch, 2019. "How Mass Surveillance Works in Xinjiang, China". *The Human Rights Watch.* https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang

Ibekwe N., 2015. "Over N121 billion wasted, Nigeria's troubled National ID Card project in fresh controversy". *Premium Times.* https://www.premiumtimesng.com/news/headlines/183720-over-n121-billion-wasted-nigerias-troubled-national-id-card-project-in-fresh-controversy.html

Ibukun Y., 2018. "China Exim Bank Loans $328 Million for Nigerian Internet Project". *Bloomberg*. https://www.bloomberg.com/news/articles/2018-09-01/china-exim-bank-loans-328-million-for-nigerian-internet-project

IDEA, 2017. "ICTs in Elections Database- Voter registration and identification". *Institute for Democracy and Electoral Assistance.* https://www.idea.int/data-tools/question-countries-view/738/Africa/cnt

Isaac M., 2019. "Facebook Finds New Disinformation Campaigns and Braces for 2020 Torrent". *The New York Times.* https://www.nytimes.com/2019/10/21/technology/facebook-disinformation-russia-iran.html

Itimu K., 2018. "eCitizen and Other Popular Kenyan Websites are not Secure- Report". *Techweez.* https://techweez.com/2018/07/24/ecitizen-popular-kenyan-websites-not-secure-report/

ITWeb, 2016. "Nigeria: Electoral Commission accused of data security blunder". *ITWeb.* https://itweb.africa/content/nWJadMbeNYl7bjO1

Iwanek K., 2018. "WhatsApp, Fake News? The Internet and Risks of Misinformation in India." *The Diplomat*. https://thediplomat.com/2018/07/whatsapp-fake-news-the-internet-and-risks-of-misinformation-in-india/

Karabus J., 2019. "Charmin'. Garmin admits customers' full credit card data nicked from South African web store". *The Register*. https://www.theregister.co.uk/2019/09/13/garmin_breach_notification/

Katwala A., 2019. "The Race to Create a Perfect Lie Detector – and the Dangers of Succeeding," *The Guardian.* https://www.theguardian.com/technology/2019/sep/05/the-race-to-create-a-perfect-lie-detector-and-the-dangers-of-succeeding

Kaye D., 2015. "Report on encryption, anonymity, and the human rights framework". United Nations Human Rights Council. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

Kayser-Bril N., 2019. "Identity-management and citizen scoring in Ghana, Rwanda, Tunisia, Uganda, Zimbabwe and China". *AlgorithmWatch.* https://algorithmwatch.org/wp-content/uploads/2019/10/Identity-management-and-citizen-scoring-in-Ghana-Rwanda-Tunesia-Uganda-Zimbabwe-and-China-report-by-AlgorithmWatch-2019.pdf

KeepItOn, 2018. "The State of Internet Shutdowns Around the World". KeepItOn. https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf

Kenya National Commission on Human Rights, 2017. "Alternative Report to the Committee on Elimination of All Forms of Racial Discrimination". https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/KEN/INT_CERD_IFN_KEN_27238_E.pdf

Khamadi S., 2017. " Paul Odhiambo arrested for 'publishing inflammatory messages' on Facebook". *iFree*. https://www.ifree.co.ke/2017/07/paul-odhiambo-arrested-publishing-inflammatory-messages-facebook/

Kornbluh K., Goodman E., and Weiner E., 2020. "Safeguarding Democracy Against Disinformation". *German Marshall Fund of the United States.* http://www.gmfus.org/publications/safeguarding-democracy-against-disinformation?utm_source=email&utm_medium=email&utm_campaign=ww%202020-03-25

Kramer F., 2019. "Fact-checking in Africa". *Konrad-Aenauer-Stiftung*. https://www.kas.de/en/web/medien-afrika/veranstaltungsberichte/detail/-/content/fact-checking-in-africa

Kwet M., 2019. "Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa". *Vice News*. https://www.vice.com/en_us/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa

Lee J., 2017. " Laxton Group to supply biometric voter registration kits for Zimbabwe elections". *BiometricUpdate.* https://www.biometricupdate.com/201706/laxton-group-to-supply-biometric-voter-registration-kits-for-zimbabwe-elections

Link J., 2019. "How Huawei could survive Trump". *The Washington Post.* https://www.washingtonpost.com/politics/2019/06/10/what-do-we-know-about-huaweis-africa-presence/

Lohr S., 2018. "Facial Recognition Is Accurate If You're A White Guy". *The New York Times.* https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Madianou M., 2019. "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies". *Television and New Media.* https://journals.sagepub.com/doi/abs/10.1177/1527476419857682

Madowo L., 2018. "How Cambridge Analytica poisoned Kenya's democracy". *The Washington Post.* https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/

Malalo H. and Mohammed O., 2018. "Kenya's president signs cybercrimes law opposed by media rights groups". *Reuters.* https://www.reuters.com/article/us-kenya-lawmaking/kenyas-president-signs-cybercrimes-law-opposed-by-media-rights-groups-idUSKCN1IH1KX

Martin-Rozumilowicz B. and Kuzel R., 2019. "Social Media, Disinformation and Electoral Integrity". *International Foundation for Electoral Systems.* https://www.ifes.org/sites/default/files/ifes_working_paper_social_media_disinformation_and_electoral_integrity_august_2019_0.pdf

Masood E., 2019. " How China is redrawing the map of world science". *Nature.* https://www.nature.com/immersive/d41586-019-01124-7/index.html

Mayhew S., " Ugandan police deploy Gemalto tech for rapid capture of suspects' biometric data". *Biometric Update.* https://www.biometricupdate.com/201902/ugandan-police-deploy-gemalto-tech-for-rapid-capture-of-suspects-biometric-data

Miriri D., 2020. "Kenya's Safaricom to consider Huawei as supplier for 5G network". *Reuters.* https://www.reuters.com/article/us-kenya-safaricom/kenyas-safaricom-to-consider-huawei-as-supplier-for-5g-network-idUSKBN20E1RG

Moore J., 2018. "Cambridge Analytica Had a Role in Kenya Election, Too". *The New York Times.* https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html

Mosk M., Turner T., and Faulders K., 2018. "Russian influence operation attempted to suppress black vote: Indictment". *ABC News.* https://abcnews.go.com/Politics/russian-influence-operation-attempted-suppress-black-vote-indictment/story?id=53185084

Moss S., 2019. "Huawei to build Konza data center and smart city in Kenya, with Chinese concessional loan". *Data Center Dynamics.* https://www.datacenterdynamics.com/en/news/huawei-build-konza-data-center-and-smart-city-kenya-chinese-concessional-loan/

Mozur P., 2019. "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority". *The New York Times.* https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Mozur P. and Krolik A., 2019. "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers". *The New York Times.* https://www.nytimes.com/2019/12/17/technology/china-surveillance.html

Munshi N., 2020. "Africa's cloud computing boom created data centre gold rush". *Financial Times.* https://www.ft.com/content/402a18c8-5a32-11ea-abe5-8e03987b7b20

Muthuri R., Monyango F., and Karanja W., 2018. "Biometric technology, elections, and privacy: Investigating privacy implications of biometric voter registration in Kenya's 2017 Election Process." Centre for Intellectual Property and Information Technology Law. https://www.cipit.org/images/downloads/CIPIT-Elections-and-Biometrics-Report.pdf

Mutung'u G., 2018. "The Influence Industry Data and Digital Election Campaigning in Kenya". *Tactical Technology Collective.* https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

National Coalition of Human Rights Defenders of Kenya, 2018. "Stop Watching Me". *Privacy International.* https://issuu.com/nchrd-k/docs/edited_nchrd_survey_report

National Coalition of Human Rights Defenders of Kenya, 2019. "The Right to Privacy in Kenya". *Privacy International.* https://privacyinternational.org/sites/default/files/2019-12/The%20Right%20to%20Privacy%20in%20Kenya_35%20UPR%20session.pdf

Nirkin Y., Keller Y., and Hassner T., 2019. "FSGAN: Subject Agnostic Face Swapping and Reenactment" arXiv. https://arxiv.org/pdf/1908.05932.pdf

NITDA, 2019. "Nigeria Data Protection Regulation". https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf

Nyabola N., 2017. "Texts, Lies, and Videotape". *Foreign Policy.* https://foreignpolicy.com/2017/08/01/texts-lies-and-videotape-kenya-election-fake-news/

Nyabola N., 2018. "In Kenya, Election Manipulation Is a Matter of Life and Death". *The Nation.* https://www.thenation.com/article/archive/in-kenya-election-manipulation-is-a-matter-of-life-and-death/

Nyabola N., 2019. "Digital Democracy, Analogue Politics: How the Internet Era Is Transforming Politics in Kenya". *Foreign Affairs.* https://www.foreignaffairs.com/reviews/capsule-review/2019-08-12/digital-democracy-analogue-politics-how-internet-era-transforming

Nyabola N., 2020. "Cambridge Analytica and the end of elections". *Al Jazeera.* https://www.aljazeera.com/indepth/opinion/cambridge-analytica-elections-200112201424047.html

O'Brien D., 2019. "Massive Database Leak Gives Us a Window into China's Digital Surveillance State". *EFF.* https://www.eff.org/fr/deeplinks/2019/03/massive-database-leak-gives-us-window-chinas-digital-surveillance-state

Obulutsa G., 2017. " Kenya president's election campaign used firm hired by Trump: privacy group". *Reuters.* https://www.reuters.com/article/us-kenya-politics/kenya-presidents-election-campaign-used-firm-hired-by-trump-privacy-group-idUSKBN1E82QS

ODSC - Open Data Science, 2019. "FSGAN: Subject Agnostic Face Swapping and Reenactment," *Medium.* https://medium.com/@ODSC/fsgan-subject-agnostic-face-swapping-and-reenactment-2f033b0ea83c

Ojekunle A., 2019. "President Buhari has rejected a bill seeking to protect the rights of internet users in Nigeria from infringement". *Pulse.* https://www.pulse.ng/bi/politics/buhari-rejects-digital-rights-bill-a-bill-seeking-to-protect-the-rights-of- internet/zztwxz1

Okeyo A., 2018. "From African American Voters to African Nations, Cambridge Analytica Wages 'Cultural Warfare". *The Progressive.* https://progressive.org/dispatches/from-african-american-voters-to-african-nations-cambridge-analytica-180521/

Oxygen Forensics, 2019. "Detective 11.5". Oxygen Forensics. https://www.oxygen-forensic.com/uploads/press_kit/OF_RN_11_5_web.pdf

Page J., O'Keeffe K., Taylor R., 2019. " America's Undersea Battle With China for Control of the Global Internet Grid". *The Wall Street Journal.* https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466

Paradigm International, 2018. "The Right to Privacy in Nigeria". *Privacy International.* https://www.privacyinternational.org/sites/default/files/2018-05/UPR_The%20Right%20to%20Privacy_Nigeria.pdf

Parkinson J., Bariyo N., and Chin J., 2019. "Huawei Technicians Helped African Governments Spy on Political Opponents". *The Wall Street Journal.* https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

Pauwels E., 2018. "China is pushing hard to overtake Silicon Valley and win the biotech race, and gain control of the world's biological data". *South China Morning Post.* https://www.scmp.com/comment/insight-opinion/united-states/article/2174533/china-pushing-hard-overtake-silicon-valley-and

Pauwels E., 2019. "The New Geopolitics of Converging Risks". United Nations University. https://collections.unu.edu/eserv/UNU:7308/PauwelsAIGeopolitics.pdf

Poetranto I., 2013. "Paradigm Initiative Nigeria Seeks Information on Surveillance Systems in Nigeria". *The Citizen Lab, University of Toronto.* https://citizenlab.ca/2013/10/the-cyber-stewards-network-speak-out-on-prism/

Poonam S. and Bansal S., 2019. "Misinformation Is Endangering India's Election". *The Atlantic.* https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/

Posetti J., Simon F., and Shabbir N. "Reporting elections on the frontline of the disinformation war". *Reuters Institute.* https://reutersinstitute.politics.ox.ac.uk/risj-review/reporting-elections-frontline-disinformation-war

Prasso S., 2019. "China' Silk Road is Looking More Like an Iron Curtain", *Bloomberg.* https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain

Privacy International, 2017. "Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism In Kenya". *Privacy International.* https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya

Privacy International, 2017b. "Voter Profiling in the 2017 Kenyan Election". *Privacy International.* https://privacyinternational.org/blog/845/voter-profiling-2017-kenyan-election

Privacy Interanational, 2018. "Further questions on Cambridge Analytica's involvement in the 2017 Kenyan Elections and Privacy International's investigations". *Privacy International.* https://privacyinternational.org/long-read/1708/further-questions-cambridge-analyticas-involvement-2017-kenyan-elections-and-privacy

Privacy International, 2019a. "State of Privacy Kenya". *Privacy International.* https://privacyinternational.org/state-privacy/1005/state-privacy-kenya

Privacy International, 2019b. "Africa: SIM Card Registration Only Increases Monitoring and Exclusion". *Privacy International.* https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion

Privacy International, 2019c. " Inside Niger's New Biometric Voting System". *Privacy International.* https://privacyinternational.org/long-read/3273/case-study-biometric-voting-cards

Privacy International, 2019d. "Myanmar: Dangerous Plans for Biometric SIM Card Registration Must be Scrapped". *Privacy International.* https://privacyinternational.org/news-analysis/3303/myanmar-dangerous-plans-biometric-sim-card-registration-must-be-scrapped

Privacy International, 2020a. "2020 is a crucial year to fight for data protection in Africa". *Privacy International.* https://www.privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa

Privacy International, 2020b. "The Hindsight Files 2020: Much More Than Politics". *Privacy International.* https://privacyinternational.org/news-analysis/3343/hindsight-files-2020-much-more-politics

Privacy International, 2020c. "Analysis of Kenya's Data Protection Act, 2019". *Privacy International.* https://privacyinternational.org/advocacy/3348/analysis-kenyas-data-protection-act-2019

Rankin J., 2020. "Russian media 'spreading Covid-19 disinformation". *The Guardian.* https://www.theguardian.com/world/2020/mar/18/russian-media-spreading-covid-19-disinformation

Republic of Kenya, 2018. "The Computer Misuse and Cybercrimes Act, 2018". http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

Republic of Nigeria, 2015. "Cybercrimes Bill". https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

Rodny-Gumede Y., 2017. "Fake news: the internet has turned an age-old problem into a new threat". *The Conversation.* http://theconversation.com/fake-news-the-internet-has-turned-an-age-old-problem-into-a-new-threat-72111

Roussi A., 2019. " Chinese investments fuel growth in African science". *Nature.* https://www.nature.com/immersive/d41586-019-01398-x/index.html

Schulze E., 2019. "Russia just brought in a law to try to disconnect its internet from the rest of the world". *CNBC.* https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html

Schwirtz M. and Borgia G., 2019. "How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader". *The New York Times.* https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html

SecurityToday, 2018. "Biometrics Market to Hit $50 Billion by 2024". *SecurityToday.* https://securitytoday.com/articles/2018/02/08/biometrics-market-to-hit-50-billion-by-2024.aspx?admgarea=ht.emergingtechnologies&m=1

Segal D., 2018. "How Bell Pottinger, P.R. Firm for Despots and Rogues, Met Its End in South Africa". *The New York Times.* https://www.nytimes.com/2018/02/04/business/bell-pottinger-guptas-zuma-south-africa.html

Shahbaz A., 2018. "The Rise of Digital Authoritarianism". *Freedom House.* https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Shen Q., 2019. "China Will Likely Corner the 5G Market—and the US Has No Plan". *Wired.* https://www.wired.com/story/china-will-likely-corner-5g-market-us-no-plan/

Prasso S., 2019. "China' Silk Road is Looking More Like an Iron Curtain." *Bloomberg.* https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain

Shi-Kupfer K. and Ohlberg M., 2019. "China Digital Rise". *Mercator Institute for China Studies.* https://www.merics.org/sites/default/files/2019-04/MPOC_No.7_ChinasDigitalRise_web_4.pdf

Singer N, 2019. "Amazon Is Pushing Facial Technology That a Study Says Could Be Biased". *The New York Times.* https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html

Singer P., Wood P., and Stone A., 2020. "How China Is Working to Quarantine the Truth About the Coronavirus". *Defense One.* https://www.defenseone.com/ideas/2020/02/how-china-working-quarantine-truth-about-coronavirus/162985/

Solomon S., 2018. "Cambridge Analytica Played Roles in Multiple African Elections ". *VOA News.* https://www.voanews.com/africa/cambridge-analytica-played-roles-multiple-african-elections

Stupp C., 2019. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case". *The Wall Street Journal.* https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Tactical Tech, 2019. "Personal Data: Political Persuasion Inside the Influence Industry. How it works". *Tactical Tech.* https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf

Telford T., 2019. "'Emotion detection' AI is a $20 billion industry. New research says it can't do what it claims." *The Washington Post.* https://www.washingtonpost.com/business/2019/07/31/emotion-detection-ai-is-billion-industry-new-research-says-it-cant-do-what-it-claims/

Theodorou Y., Okong'o K., and Yongo E., 2019. Access to Mobile Services and Proof of Identity 2019. *GSMA.* https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf

Tonisi L., 2019. "Fake news monitor launched for 2019 election season". *Daily Maverick.* https://www.dailymaverick.co.za/article/2019-04-02-fake-news-monitor-launched-for-2019-election-season/

Tucker P., 2019. "The West Isn't Ready for the Coming Wave of Chinese Misinformation: Report". *Defense One.* https://www.defenseone.com/technology/2019/03/researcher-west-isnt-ready-coming-wave-chinese-misinformation/155400/

UK Parliament Select Committee on Culture, Media, and Sport, 2018. "Disinformation and 'fake news': Interim Report". *UK Parliament.* https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36309.htm

Umematsu T., Sano A., and Picard R., 2019. "Daytime Data and LSTM can Forecast Tomorrow's Stress, Health, and Happiness,". *41st International Engineering in Medicine and Biology Conference.* https://www.media.mit.edu/publications/daytime-data-and-lstm-can-forecast-tomorrow-s-stress-health-and-happiness/

United Nations General Assembly, 2019. "General Assembly Approves $3.07 Billion Programme Budget as It Adopts 22 Resolutions, 1 Decision to Conclude Main Part of Seventy-Fourth Session". https://www.un.org/press/en/2019/ga12235.doc.htm

UN Human Rights Council, 2019. "Surveillance and human rights". *United Nations Digital Library*. https://digitallibrary.un.org/record/3814512?ln=en

UN Human Rights Office, 2019. "Cooperation Agreement". https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25010&LangID=E

UN Human Rights Office, 2019b. "The 2019 report on the surveillance industry ". United Nations. https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx

van Zyl G., 2017. "Biggest ever SA data breach: 60 million ID numbers leaked on real estate server". *BizNews*. https://www.biznews.com/global-citizen/2017/10/20/biggest-ever-sa-data-breach

Ward C., Polglase K., Shukla S., Mezzofiore G., and Lister T., 2020. "Russian election meddling is back -- via Ghana and Nigeria -- and in your feeds". *CNN*. https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html

Wardle C., Derakhshan H., 2017. "Information Disorder: Toward an interdisciplinary framework for research and policymaking". *Council of Europe.* https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Wasuna B., 2018. "How rogue IEBC staff minted cash from sale of voters' data". *The Star*. https://www.the-star.co.ke/news/2018-05-10-how-rogue-iebc-staff-minted-cash-from-sale-of-voters-data/

Weinberger S., 2019. "Private Surveillance Is a Lethal Weapon Anybody Can Buy". *The New York Times*. https://www.nytimes.com/2019/07/19/opinion/private-surveillance-industry.html

Winder D., 2019. "A 'Government Database' Of 92 Million Citizen Records For Sale To Highest Bidder." *Forbes*. https://www.forbes.com/sites/daveywinder/2019/10/06/a-government-database-of-92-million-citizen-records-for-sale-to-highest-bidder/#47c572ea701b

Woodhams S., 2019. "How China Exports Repression to Africa". *The Diplomat.* https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/

York G., 2018. "Cambridge Analytica parent company manipulated Nigeria's 2007 election, documents show". *The Globe and Mail.* https://www.theglobeandmail.com/world/article-cambridge-analytica-parent-company-manipulated-nigerias-2007-election/

© 2015, Kenya. UNHCR aid for those displaced by post-election violence

**Konrad-Adenauer-Stiftung e. V.**

Andrea E. Ostheimer
Executive Director
www.kas.de/newyork

andrea.ostheimer@kas.de