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.

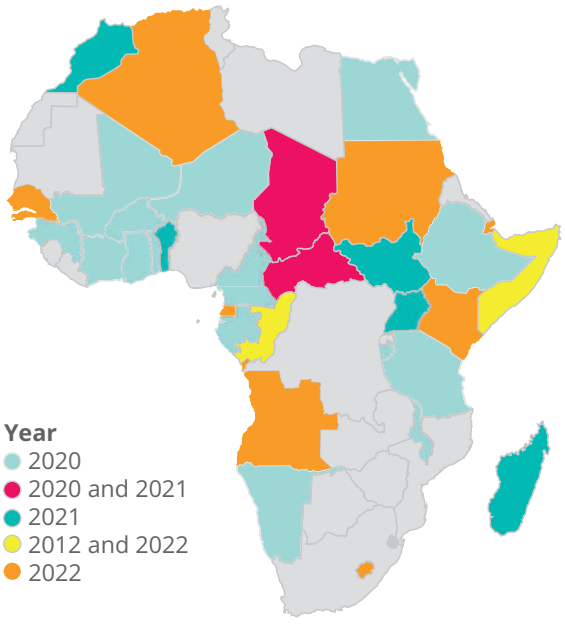
The global development agenda seeks to realize the promises of the digital economy, bringing prosperity, inclusion and empowerment. Biometric and digital ID systems are making exponential advances across the African continent, with many nations in the process of registering their populations' biometrics 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.

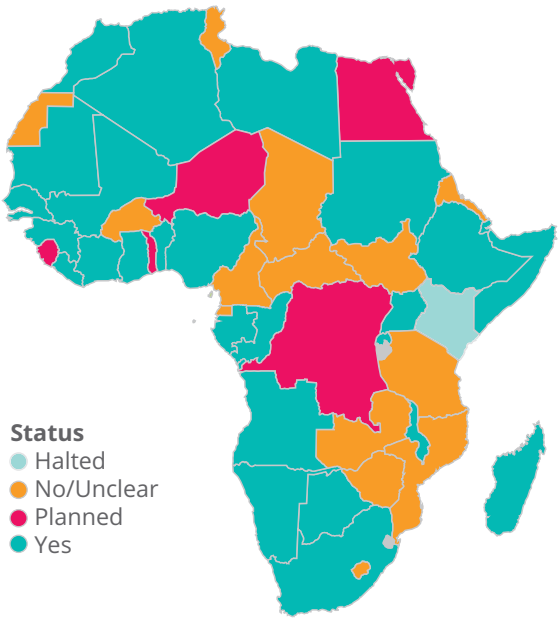
Converging technologies monitor and analyse individuals' biometrics and behavioural data, gradually imposing social and political control over those individuals' lives. Such "power over life" resonates with what French philosopher, Michel Foucault, termed *biopower*: "[A] power that exerts a positive 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.

Konrad-Adenauer-Stiftung e. V.

Andrea E. Ostheimer
Executive Director
www.kas.de/newyork

andrea.ostheimer@kas.de