Africa in the Crosshairs of New Disinformation and Surveillance Schemes That Undermine Democracy

Dec 9, 2019 0 comments

By Daniel Mwesigwa |

A range of spyware vendors including Italian Hacking Team, the Anglo-German Gamma Group, and Israeli's NSO Group, have found a ready market in authoritarian and repressive governments in Africa and elsewhere. Similarly, systematic propaganda campaigns designed by meddlesome actors – including government agents and ambitious data analytics companies such as Cambridge Analytica working on behalf of state and non-state actors – are becoming conspicuous in Africa, especially during electoral periods.

The tools and tactics of these operators, who are mostly non-African, are increasingly undermining democracy and respect for human rights in Africa, as they enable mass surveillance and disinformation that manipulates and undermines political discourse.

For example, Chinese tech giant Huawei and its technicians were implicated in an August 15, 2019 exposé by The Wall Street Journal that detailed how the company's staff had helped the Uganda Police to hack into the encrypted communications of an opposition figure. As a result, the security officers were able to thwart the opposition leader's mobilisation plans. The article also stated that technicians from Huawei had helped Zambian authorities to access the phones and social media pages of a group of opposition bloggers who were tracked and arrested.

Through security vulnerabilities, spyware tools and products give governments, notably intelligence and law enforcement authorities, super powers to surveil using covert intrusion systems across major mobile platforms and operating systems. In 2016, the Citizen Lab, an interdisciplinary lab working at the intersection of global affairs and technology at the University of Toronto, uncovered Pegasus – a sophisticated malware developed by the NSO Group that is injected into a target's phone via text or WhatsApp, a popular messaging tool in Africa. The Citizen Lab has since identified Pegasus operations in over 45 countries including Algeria, Egypt, Ivory Coast, Kenya, Morocco, Rwanda, South Africa, Togo, Uganda, and Zambia. But NSO has reportedly bragged time and again how it can penetrate various operating systems and applications irrespective of the security patches.

According to the 2019 State of Internet Freedom in Africa Report, the "surveillance state" in Africa gained notoriety at the turn of the decade, after the infamous Arab Spring that swept across North Africa in 2011, allegedly amplified by dissident voices on social media. The report documents how repressive states such as Tanzania, Uganda, Ethiopia, Botswana, and Rwanda have since boosted their surveillance capabilities through procurement of advanced spyware. In 2015, it was revealed that Uganda and Tanzania had procured Hacking Team's premium Remote Control System (RCS) for intrusion into systems across major mobile platforms and operating systems.

More recently, the Financial Times reported that Rwanda paid up to USD 10 million to the NSO Group to spy on government critics and dissidents through WhatsApp – an allegation Rwanda president Paul Kagame denied in a presidential press briefing held on November 8, 2019, only acknowledging that they spy on "our enemies" using "human intelligence". He added, "I wouldn't spend my money over a nobody [Rwandan exiles] yet we have sectors like education to spend such money".

But Kagame's denial is to be taken with a pinch of salt. In 2016, a Rwandan court sentenced a popular singer, Kizito Mihigo, to 10 years in prison on allegations of conspiracy to overthrow the government, based on hacked private WhatsApp and Skype messages exchanged with alleged dissidents in exile.

The alleged Rwanda cases appear to be linked to others of NSO infiltrating the WhatsApp accounts of journalists, human rights activists, political dissidents, prominent female leaders, and other members of civil society in up to 20 countries, which prompted Facebook (the owners of WhatsApp) to sue NSO in October 2019. The lawsuit brought by Facebook in the U.S Federal Court accuses the spyware maker of hacking into the WhatsApp accounts of 1,400 users worldwide. While there are scanty details on the exact identities of the affected, it is reported that 174 are lawyers, journalists, human rights defenders and religious leaders.

According to the Financial Times, those targeted in Rwanda, six of whom it interviewed and they confirmed being alerted by WhatsApp about the possible NSO-enabled surveillance of their communications. These included a journalist living in exile in Uganda, who had petitioned the Uganda government "to help protect Rwandans in the country from assassination"; South Africa and UK-based senior members of the Rwanda National Congress (RNC), an opposition group in exile; an army officer who fled Rwanda in 2008 and testified against members of the Rwandan government in a French court in 2017; and a Belgium-based member of the FDU-Inkingi opposition party.

Meanwhile, some foreign powers are purportedly testing, as New York Times recently reported, "New Disinformation Tactics in Africa to Expand Influence". The report detailed how the Wagner Group founded by businessman Yevgeny Prigozhin, who allegedly has close ties to the Russian government, has over the last couple of years been running aggressive disinformation campaigns on Facebook.

It is reported that Prigozhin's campaign used locally-opened Facebook accounts to disguise behaviour and also used sham news networks that regularly reposted articles from Russia's state-owned Sputnik news organisation to promote Russian policies while undermining US and French policies in Africa. On October 31, 2019, Facebook reportedly removed these accounts that were influencing operations "in the domestic politics" of eight African countries – Cameroon, the Central African Republic, Congo Brazzaville, Ivory Coast, Madagascar, Mozambique, and Sudan.

Earlier in 2019, Facebook reportedly shut down a separate "fake news" operation targeting elections in African countries such as Nigeria, Senegal, Togo, Niger, Angola, and Tunisia, propagated by "inauthentic" accounts on Facebook and Instagram run by Israeli commercial firm, Archimedes Group. Between 2013 to 2017, governments such as Kenya and Nigeria reportedly hired Cambridge Analytica to manipulate their electorate in a bid to win presidential elections for the incumbents.

Besides the disinformation campaigns linked to Russian actors, and the Israel-made spyware, there are also facial recognition surveillance programmes such as the Huawei's "Smart Cities", which has been deployed in 12 African countries. This phenomenon is referred to by some as an export of digital authoritarianism.

It is now evident that governments and non-state actors face an uphill task of combatting the governance challenges caused by this phenomenon. Accordingly, governments, with the help of tech platforms, need to understand what legislation and policies, including oversight and enforcement mechanisms, are necessary to strengthen the protection of democracy and human rights in the rapidly changing digital world.

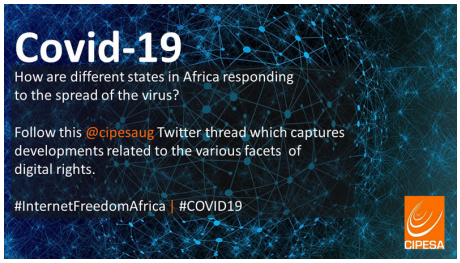
Tagged as: kenya, Rwanda, surveillance, Tanzania, Uganda

You may also like ...

ANNOUNCING THE CIPESA 2020 FELLOWS

COALITION OF CIVIL SOCIETY GROUPS LAUNCHES TOOL TO TRACK RESPONSES TO DISINFORMATION IN SUB SAHARAN AFRICA

AFRICAN INTERNET RIGHTS ALLIANCE (AIRA) DENOUNCES RESTRICTIONS ON FREEDOMS IN KENYA AND NIGERIA



The Africa Digital Rights Fund/ Le Fonds Africain pour les Droits Numériques

The Africa Digital Rights Fund offers flexible and rapid response grants to select initiatives in Africa to implement activities that advance digital rights… *Read More>>*

Featured Publications

État Des Libertés Sur Internet 2019au Sénéga

État Des Libertés Sur Internet 2019au Tchad1

État Des Libertés Sur Internet 2019au Cameroun

#FIFAfrica19 Updates

#InternetFreedomAfrica

- Building Capacity and Collaborations for Digital Rights Research in Africa
- Report: African Countries Broadening Control Over the Internet
- #FIFAfrica19: Just Days Away

Promoting Online Freedoms in Africa

OpenNet Africa

- CIPESA Joins Call Urging Burundi Gov't To #KeepItOn During Elections
- How Technology is Aiding the Covid-19 Fight in Africa
- Covid-19 in Africa: When is Surveillance Necessary and Proportionate?

ICT4Democracy in East Africa Network

- 'People With Disabilities Left Out in ICT Jamboree'
- How Nigeria and Uganda are Faring on the Right to Information

Supported by:

- Call for Evaluation Consultant: ICT4Democracy in East Africa Network

Open Data & RTI

- Leveraging ICT to Promote the Right to Information in Uganda: Insights from Ask Your Government Portal
- Access to Public Information in Uganda: Rhetoric or Reality?
- The Right To information in Uganda: Unclogging The Bottlenecks

ICT Analytics

- Why Access to Information on Covid-19 is Crucial to Persons with Disabilities in Africa
- Centre for Human Rights and CIPESA Conduct Study on Civil Society in the Context of the Digital Age in Africa
- Building Capacity and Collaborations for Digital Rights Research in Africa

Internet Governance

- Announcing the CIPESA 2020 Fellows
- Coalition of Civil Society Groups Launches Tool to Track Responses to Disinformation in Sub Saharan Africa
- African Internet Rights Alliance (AIRA) Denounces Restrictions on Freedoms in Kenya and Nigeria

CIPESA on Twitter

Tweets by cipesaug

Previous: Kenya, Tanzania and Uganda Must Do More to Improve Access to ICT for Persons with Disabilities

Next: Building Digital Literacy and Security Capacity of Women Refugees in Uganda

Archives

Select Month

Subscribe

Email

Get Updates!

YouTube Channel

Hub Cities: Emergency Me...

Upcoming Events

- EGOV-CeDEM-ePart 2020

August 31 – September 2

- Africa Future Summit 2020

September 18

- Forum on Internet Freedom in Africa 2020

September 28 – September 30