Foreign Influence on Civic Space in Uganda: Implications for Digital Rights

May **2024**

CIPESA

Introduction

Uganda is experiencing a democratic regression characterised by the declining state of press freedom, hostility towards the political opposition and critics by state agencies, and mounting restrictions on the activities of civil society organisations (CSOs). Journalists continue to face state curtailment of their constitutionally protected rights and freedoms, including through intimidation, harassment, assault, arrests and detention.[1] As a result, the situation in Uganda has been classified as "difficult" by the 2024 World Press Freedom Index produced by Reporters Without Borders. The 2024 Freedom in the World report categorises Uganda as "Not Free" based on serious concerns about the state of political rights and civil liberties.[2] The Economic Intelligence Unit's 2023 Democracy Index[3] classifies Uganda as a "hybrid regime"[4] with a rank of 99th out of 167 countries assessed.

Democracy Index ranks Uganda 99th out of 167 countries assessed

Regarding digital rights, a 2023 assessment by Freedom on the Net designated Uganda as Partly Free, scoring 51 out of 100. Repressive laws governing the digital civic space and surveillance, particularly those that enable internet censorship, network disruptions, deployment of surveillance technologies such as spyware and video surveillance, and information manipulation through government-supported disinformation campaigns, are a key concern. Problematic laws include the Computer Misuse Act 2011 and its 2022 amendment, the Regulation of Interception of Communications Act 2010, the Anti-Terrorism Act of 2002 (as amended in 2015, 2016, and 2017), the Uganda Communications Act 2013, and the Public Order Management Act 2013.

1 *HRNJ, Press Freedom Index Report – 2022: Uganda Uncertain Future for the Media, https://hrnjuganda.org/?wpdmpro=press-freedom-index-2022-uncertain-future-for-the-media&wpdmdl=9729&refresh=665878721a38c1717074034*

2 *Freedom House, Freedom in the World 2024: Uganda, https://freedomhouse.org/country/uganda/freedom-world/2024*

3 *Economic Intelligence Unit's Democracy Index 2023, https://www.eiu.com/n/democracy-index-conflict-and-polarisation-drive-a-new-low-for-global-democracy/*

4 *Elections have substantial irregularities that often prevent them from being both free and fair. Government pressure on opposition parties and candidates may be common. Serious weaknesses are more prevalent than in flawed democracies—in political culture, functioning of government and political participation. Corruption tends to be widespread and the rule of law is weak. Civil society is weak. Typically, there is harassment of and pressure on journalists, and the judiciary is not independent.*

In a globally interconnected world where geo-political interests transcend national and continental boundaries, practices in one country can have a notable effect on the laws and practices of another. Countries that do not have significant resources to finance their digital infrastructure often rely on foreign support to facilitate the construction and operation of digital technologies. In Uganda's case, China has been one of the foreign sources of support in developing digital communication and other infrastructure, including the setting up of a video surveillance system. It has also organised numerous study tours for Ugandan officials and journalists that are centred on popularising its economic and governance systems.

Perhaps not surprisingly, Uganda has mirrored some practices from China, which various respected global indices consider a leading player in digital authoritarianism and curtailing citizens' rights via technology.[5] While it is not patently clear whether China has directly influenced legislation and practice in Uganda, it has arguably inspired some of the legal frameworks and practices that fuel digital authoritarianism in the east African country. A study among Ugandans shows that their perceptions of China are largely neutral and positive, and of a benevolent nation ("despite local concerns about China's lack of transparency in its procurement processes, its marginalisation of local companies, and the low quality of its products").[6] Uganda's president, Yoweri Kaguta Museveni, has praised China for offering loans and investments without attaching conditions on governance[7]

This brief aims to illuminate how China and its model of governance and state surveillance may be influencing or inspiring retrogressive laws and undermining digital rights in Uganda. It seeks to inform awareness-raising and advocacy engagements with legislators, civil society organisations, human rights defenders (HRDs), and journalists. It also offers insights into the possible legal reforms necessary to advance digital rights in Uganda.

5 Freedom House, Freedom in the World 2024: China, https://freedomhouse.org/country/china/freedom-world/2024; Freedom on the Net: China, https://freedomhouse.org/country/china/freedom-net/2023 and Economic Intelligence Unit's Democracy Index 2023, https://www.eiu.com/n/democracy-index-conflict-and-polarisation-drive-a-new-low-for-global-democracy/

6 Nassanga, G. L., & Makara, S. (2015). Perceptions of Chinese presence in Africa as reflected in the African media: case study of Uganda. Chinese Journal of Communication, 9(1), 21–37. https://doi.org/10.1080/17544750.2015.1078386

7 Alex Otto, President Museveni Defends Chinese Loans, URN, October 9, 2019, https://ugandaradionetwork.net/story/president-museveni-defends-chinese-loans?districtId=545

China's Influence on Uganda's **Digital Rights Landscape**

There is no evidence to suggest that China applies direct coercion to influence Uganda's laws and practices related to digital rights. However, as part of the Asian country's "norm entrepreneurship", it sponsors Uganda government officials and journalists for study visits to China and facilitates content distribution by Chinese state media to popularise its systems, including in the governance arena.[8]

Indeed, there is considerable evidence that suggests the country is keen on exporting its model of governance that is characterised as authoritarian on global democracy indices. Some observers contend that the practice of silencing dissent, arresting, and detaining critics is "attractive to autocratic African countries and leaders who are persuaded that the China authoritarian model should be emulated as a means for achieving political stability as a prerequisite for economic growth."[9] Moreover, there is a common refrain that China is promoting its internet model, which includes censorship and restrictions, through digital investments in African countries.[10] Other evidence suggests that African autocracies are exploiting the adoption of China's model of the internet to roll back democratic gains through surveillance and censorship of civil liberties.[11]

China invested
USD 110
million in Uganda's
National Backbone Data Transmission Project

It must be noted, however, that evidence that claims China is actively seeking to export its governance model and influencing local laws and practices in Africa is often anecdotal and inconclusive. Moreover, such claims (and, often, the evidence they advance) assume that African governments are incapable of developing home-grown systems of governance and thoughtlessly rely on models from other continents.

Between 2007 and 2015, China invested more than USD 110 million in Uganda's National Backbone Data Transmission Project.[12] Uganda has also benefited from Chinese financial support for the National Fibre-Optic Project.[13] There are suggestions that the national backbone and fibre-optic projects "are part of a digital infrastructure that has enhanced the Ugandan government surveillance capabilities that violate the right to privacy and freedom of expression." [14]

8 *See for instance, Barbara Kaija, Chinese vision to catapult growth, New Vision, August 25, 2016, https://www.newvision.co.ug/news/1433629/chinese-vision-catapult-growth-21st-century*

9 *The Centre for Human Rights, University of Pretoria, Safeguarding Information Rights in Africa-China Relations: An Assessment of Legal Subversions, 2024*

10 *Enter the dragon: The impact of China's digital authoritarianism on democracy in Africa, https://tagp.gga.org/index.php/system/article/view/53*

11 *Gariba, A. (2023). Enter the dragon: The impact of China's digital authoritarianism on democracy in Africa. The Africa Governance Papers, 1(4). Retrieved from https://tagp.gga.org/index.php/system/article/view/53*

12 *Huaxia, China signs 151 mln USD deal to expand Uganda's data backbone infrastructure, March 11, 2023, https://english.news.cn/africa/20230311/0e88d7be10f0455d9d658db457d103c6/c.html*

13 *Uganda Business News, Uganda seeks $146mn Chinese loan for national fibre-optic project, November 27, 2023, https://ugbusiness.com/2023/11/politics-policy/uganda-seeks-146mn-chinese-loan-for-national-fibre-optic-project*

14 *See for instance, Human Rights Watch, Uganda: Rights Concerns Over License Plate Tracking, November 14, 2023, https://www.hrw.org/news/2023/11/14/uganda-rights-concerns-over-license-plate-tracking#*

China has continually buttressed its influence over Uganda's social-economic development through the seemingly *no-strings-attached loan schemes* that have often been acknowledged and *praised* by President Museveni. Nevertheless, this influence comes with preconceived and predetermined perceptions of controls over existing practices to create democracies with similar governance and development models.[15] This is because China's non-interference policy in the internal affairs of other countries allows their governments greater leeway to suppress dissent and democratic processes without facing criticism or repercussions from China. By contrast, the Uganda government or senior public officials have during 2023 and 2024 attracted sanctions by the United States of America, the United Kingdom and the World Bank over governance and human rights concerns. As such, the Chinese no-governance-strings-attached model is criticised for emboldening authoritarian tendencies in the countries it partners with. This non-interference policy is now understood as a major enabler for all kinds of repression, as "it ensures that Chinese money continues to flow to potentially unsavoury African regimes, thus further entrenching authoritarian leadership where it already exists."[16]

China is renowned for "increased monitoring by digital means and laws and regulations that severely restrict individual liberties."[17] There are notable similarities in Uganda, which, besides the digital surveillance, has enacted laws that repress civil liberties and constrain the digital civic space, granting state authorities wide latitude to conduct surveillance with limited judicial or other independent oversight. Chinese companies are leading exporters of video surveillance technology, including that with facial recognition capabilities, which Uganda has acquired and deployed in manners that often compromise privacy, in the name of law enforcement, public security, and urban management.

In 2019, a Wall Street Journal reported that Huawei - a privately owned Chinese technology company - had aided security agencies to spy on President Museveni's political opponents.[18] The report showed how Huawei technicians helped Ugandan intelligence services to infiltrate encrypted communications of opposition leader Robert Ssentamu Kyagulanyi, a.k.a. Bobi Wine, and were, as a result, able to monitor his movements and scuttle his mobilisation rallies for the 2021 election.[19] There was no evidence or indication that the Chinese government directed Huawei technicians to offer surveillance assistance to Ugandan officials.

15 *Africa Intelligence, Spotlight | Uganda Frustrated Museveni finds Chinese loans come with political strings attached, December 13, 2019, https://www.africaintelligence.com/eastern-africa-and-the-horn/2019/12/13/frustrated-museveni-finds-chinese-loans-come-with-political-strings-attached,108386157-eve*

16 *A Luongo How Chinese non-interference enables African authoritarianism, Democracy in Africa http://democracyinafrica.org/how-chinese-non-interference-enables-african-authoritarianism/*

17 *Katja Drinhausen, Marina Rudyak, The Decoding China Dictionary, https://rwi.lu.se/wp-content/uploads/2021/03/Decoding-China-Publication_FINAL.pdf*

18 *Joe Parkinson, Nicholas Bariyo and Josh Chin, Huawei Technicians Helped African Governments Spy on Political Opponents, The Wall Street Journal, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.*

19 *Ibid.; See also Salem Solomon, In Uganda, Dissidents Adapt to Evade Huawei Assisted Government Spying, https://www.voanews.com/africa/uganda-dissidents-adapt-evade-huawei-assisted-government-spying*

Collaboration between the PRC [People's Republic of China] and autocratic African regimes has empowered the latter to undermine key fundamental democratic underpinnings, including access to information and freedom of expression. This is conspicuously demonstrated through the emulation of the PRC's authoritarian model, which suppresses online expression and stifles dissenting voices through the imposition of anti-online expression laws and internet shutdowns. It is presumed that companies affiliated with the PRC have played a role in facilitating these shutdowns. The global ramifications of the ties between the PRC and some African states are evident in the international arena, exemplified by the support the Chinese government has garnered from the United Nations despite concerns about human rights violations. - The Centre for Human Rights, University of Pretoria, Safeguarding Information Rights in Africa-China Relations: An Assessment of Legal Subversions, 2024.

Huawei is also the supplier of a closed-circuit television (CCTV) system in Uganda, whose deployment was purportedly aimed at promoting safety and security in public spaces.[20] There is no evidence that the CCTV, which has facial recognition functionalities, has helped to reduce crime around Uganda. Yet, as researchers have observed, the extent to which citizens' data is stored, tracked, and profiled within acceptable legal, regulatory, and ethical procedures remains unknown.[21]

As of 2024, surveillance is getting further entrenched with the introduction of digital number plates through the so-called Intelligence Transport Monitoring System (ITMS). According to Human Rights Watch, the system allows the government to track the real-time location of all vehicles in the country, thereby undermining privacy rights and creating serious risks to the rights to freedom of association and expression.[22]

The increasing surveillance in Uganda could facilitate human rights abuses, such as interference with personal privacy and curtailing freedom of expression, assembly and association, and information.[23] Indeed, a previous study found that the majority of journalists, HRDs, and activists believed that Ugandan security agencies were routinely monitoring and intercepting citizens' communications, with most surveillance activity thought to be targeted at politicians opposed to the ruling party, critical journalists, and non-government organisations (NGOs) engaged in political work.[24]

20 *Stephen Kafeero, Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests, https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/.*

21 *Artificial Intelligence and State Repression in Africa, https://thecfma.org/artificial-intelligence-and-state-repression-in-africa/*

22 *Human Rights Watch, Uganda: Rights Concerns Over License Plate Tracking, November 14, 2023, https://www.hrw.org/news/2023/11/14/uganda-rights-concerns-over-license-plate-tracking#:*

23 *State of Privacy Uganda https://privacyinternational.org/state-privacy/1013/state-privacy-uganda*

24 *CIPESA, State of Internet Freedom in East Africa 2015, https://cipesa.org/?wpfb_dl=193*

Local Laws and **Digital Rights Suppression**

Effects on Privacy and Civil Liberties: The conduct of surveillance using systems such as video surveillance, spyware and facial recognition elicit concerns about privacy infringement as well as potential abuses of power. In Uganda, the adoption of Chinese surveillance systems does not have safeguards for privacy rights and could enable government surveillance without proper oversight from parliament and courts of law. Additionally, there are risks of data misuse, including the potential to use such systems to suppress critics and opponents and to violate human rights.

Previous research has established that the tight relations between China and African governments make it difficult to identify and attribute the legal pressures that they exert in the African information system.[25] While it is impossible to state categorically that foreign influence has directly influenced Uganda's legal framework, economic and social relations between countries can facilitate the enactment of laws that regulate the digital space and the use of digital technologies. For instance, the Uganda-China economic relations have facilitated the development of ICT infrastructure, and enabled the importation and deployment of problematic technologies from the Asian country, which has had implications on Uganda's digital civic space.

It is not in doubt that Uganda's laws governing the digital domain contribute to suppression of digital rights. For instance, the Computer Misuse Act 2011 as amended in 2022, the Regulation of Interception of Communications Act of 2020, the Anti-Terrorism Act of 2002 (as amended in 2015, 2016, and 2017), the Uganda Communications Act 2013 and the Public Order Management Act 2013 provide for and create onerous obligations for the sector players including telecom companies and Internet Service Providers (ISPs) including compatibility with state monitoring apparatus and disclosure of user data.[26] The eminent result of these actions and practices is curtailment of civil liberties.

Popular, too in Uganda is the utilisation of Strategic lawsuits against public participation (also known as SLAPP suits or intimidation lawsuits), which stifle free speech, access to information, and healthy debate by targeting those who speak out on issues of public interest or criticise the government. SLAPPs are *used to silence* and harass critics by forcing them to spend money defending these baseless suits. They are intended to intimidate those who disagree with them or their activities by draining the target's financial resources. Notable SLAPP cases in Uganda include those against academic *Stella Nyanzi* for "insulting and disturbing the peace, quiet or the right to privacy of the president"; *Robert Shaka* in 2015 for "offensive communication", among several others. As earlier noted, democracy regression in China is characterised by limited space for participation and the exercise of fundamental rights and freedoms. Uganda's current SLAPP practices ogre with China's with an increasingly narrowing space for the exercise of civil liberties and rights.

25 *The Centre for Human Rights, University of Pretoria, Safeguarding Information Rights in Africa-China Relations: An Assessment of Legal Subversions, 2024.*

26 *CIPESA, State of Internet Freedom in East Africa 2021: Effects of State Surveillance on Democratic Participation in Africa, https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Africa-2021-Report.pdf*

The Nature of Digital Rights
Repression in Uganda

Below are some ways in which digital rights are suppressed in Uganda that indicate increased digital control and surveillance:

Social Media Shutdowns and Internet Censorship: On various occasions, including during the 2011, 2016 and 2021 election periods, Ugandan authorities ordered the blockage of access to social media platforms.[27] The shutdowns were purportedly intended to curtail the spread of disinformation and to demobilise protest organisers and protest goers. On the eve of the 2021 elections, Uganda ordered the blockage of access to social media. In the same year, the internet was completely shut down during the general elections.[28] As of May 2024, access to Facebook remains blocked. Uganda also censors access to Virtual Private Networks (VPNs), various news sites, and porn sites.

Surveillance Infrastructure: The Uganda government has invested in a video surveillance infrastructure, including CCTV cameras and monitoring systems that have facial recognition capabilities. According to reports, the facial recognition technology which is supplied by Huawei has been used to crack down on dissent after anti-government protests - a practice China is also known to indulge in[29]. Uganda is also in the process of rolling out the Intelligent Transport Monitoring System (*ITMS*), through which each vehicle and motorcycle will compulsorily be installed with a chip that enables authorities to pinpoint its exact location at any one time. According to Human Rights Watch, the ITMS "amounts to unchecked mass surveillance of all vehicles at all times, undermining the right to privacy for millions of Ugandans."

Some journalists and activists have also been targets of malware purportedly sponsored by state-affiliated actors. In 2012, Uganda allegedly purchased spyware called FinFisher to suppress the activities of opposition politicians through monitoring of computers and smartphones in the Fungua Macho ("open your eyes") operation.[30] The government also reportedly used spyware to bug office and residential buildings, vehicles, electronic gadgets, and business centres such as hotels to collect data and carry out surveillance. Uganda has also used the tech giant Huawei to intercept opposition politicians' communications. In December 2021, the New York Times reported that Apple had warned two Ugandan journalists and an opposition leader that their iPhones may have been infected by spyware.

27 *Frederic Musisi, Social media, Mobile Money switched off over national security concerns, Daily Monitor, February 18, 2016, https://www.monitor.co.ug/News/National/Social-media-Mobile-Money-switched-off-over/688334-3082556-fnl4xjz/index.html*

28 *Uganda Eases Internet Shutdown Imposed Over Election, https://www.capitalfm.co.ke/news/2021/01/uganda-eases-internet-shutdown-imposed-over-election/*

29 *Ibid.*

30 *Amar Toor, Uganda government used advanced spyware to 'crush' opposition, report says, The Verge Oct 16, 2015, https://www.theverge.com/2015/10/16/9549151/uganda-finfisher-surveillance-spyware-privacy-international; see also Benon Herbert Oluka, Govt Spends Shs 200bn on Spying Gadgets, The Observer, October 19, 2015, https://www.observer.ug/news-headlines/40521-govt-spends-shs-200bn-on-spying-gadgets.*

Weaponisation of Laws: Uganda has enacted laws that grant broad powers to the government to regulate and control online expression. For example, the Computer Misuse Act criminalises "offensive communication" and has been invoked to arrest various individuals for posting content that authorities consider offensive and false against the government and government officials. These laws have been used to target critics, and this silences critical voices, promotes self-censorship, and discourages citizen participation. The Regulation of Interception of Communications Act (RICA) 2010 was enacted to provide for lawful interception and monitoring of some communications in the course of their transmission. In addition, the Anti-Terrorism Act 2002 in section 19(2) authorises officers to intercept communications and carry out surveillance on individuals suspected of terrorist acts.

Most of these laws are filled with ambiguities in both provisions and scope of application. They give wide discretionary powers to agencies such as the Uganda Communications Commission, and to the heads of security agencies. They also lack clear oversight mechanisms over their implementation, which provides room for abuse in application. Furthermore, they are weak in providing for the rights of individuals as they mostly emphasise facilitating regulatory functions and controls as opposed to prioritising individuals' rights.

Disinformation: The government has been accused of utilising social and digital media for disinformation campaigns. Such campaigns, which use bots, fake accounts, and paid social media armies (some freelance, others under the government's formal employment), aim to discredit political opponents and to manipulate public opinion in favour of the government/ ruling party narratives. Days before the *2021 elections*, Twitter and Meta removed several accounts belonging to government and ruling party officials whom the social media platforms accused of coordinated inauthentic behaviour (CIB). According to Meta, CIB refers to the use of multiple Facebook or Instagram *assets working in concert* to misrepresent themselves, artificially boost the popularity of the content, or engage in behaviours designed to enable other violations under the platform's community standards, and where the use of fake accounts is central to the operation.

Recommendations

Uganda should resist all foreign influence and models that promote digital authoritarianism and undermine democracy. The country's laws must respect internationally recognised human rights standards and promote the use of a free, open, and safe internet. In view of the observed trend in the country towards building a digital autocracy, in law and in practice, the following recommendations for different stakeholders could be trajectory in the right direction.

Parliament

1. Strengthen legal and regulatory frameworks by amending or repealing regressive and oppressive frameworks to ensure responsible and ethical use of surveillance technology. Changes in the laws should provide for robust oversight by independent bodies such as the parliament and courts of law over the conduct of surveillance.

2. Engender accountability and transparency in Uganda by scrutinising government policy and administration through monitoring the implementation of Government programmes and projects, including foreign investments in technology, to ensure a human-centred and human rights-based approach in implementation.

3. Enact laws that specifically protect journalists, whistle-blowers, human rights defenders and activists from wanton threats, arrests and prosecutions over legitimate online communications and activism that advances social accountability, respect for human rights, and good governance.

Civil Society

1. Conduct evidence-based research into the actions of foreign actors and how they adversely impact local laws, policies, and democratic governance. The research should include an analysis of laws to identify problematic provisions and gaps that facilitate the repression of digital rights and make proposals for reform to stakeholders, including the parliament and line ministries.

2. Engage in proactive advocacy with Parliament to push for the amendment of contentious provisions in laws and policies relating to freedom of expression; and engage regional and international bodies and human rights mechanisms, including the United Nations, the African Union, and the East African Community, to assess Uganda's human rights record and compliance with established human rights standards.

3. Jointly with other stakeholders, including academia, the media, and lawyers, engage in public interest litigation to challenge provisions in legislation that limit the exercise of digital rights.

4. In partnership with academia, lawyers, and think tanks, consistently conduct public awareness raising about foreign influence on digital rights and democratic governance.

5. Build the capacity of journalists and other human rights defenders to investigate and effectively report on foreign malign influence and its effects on local laws and the respect for human rights and democratic governance.

Private Sector

1. Key players, including telecom companies and internet service providers, should develop privacy policies that aim to robustly protect users' privacy despite the onerous obligations such as communication interception that they owe to security agencies.

2. Adhere to the UN Guidelines on Business and Human Rights by, among others, ensuring that their actions, including those from their regulators, do not violate individuals' rights.

3. In collaboration with other stakeholders, including civil society, media, lawyers, and academia, engage in litigation to challenge regressive provisions in laws that curtail or limit the exercise of digital rights and freedoms or that are wantonly intrusive of individual privacy.

4. Proactively publish transparency reports on cases of cooperation and disclosure with state actors so as to build confidence and trust amongst the public on the extent of adherence to their privacy standards.

Media

1. Conduct and publish investigative stories on foreign malign influence on digital rights and democratic governance. The stories should be packaged and published in a variety of formats and platforms (mainstream, electronic, and online) in order to reach different audiences.

2. Collaborative with other stakeholders, including civil society, lawyers, and academia to support litigation to challenge regressive provisions in laws that limit the exercise of digital rights by providing coverage to ongoing litigation efforts.

3. In partnership with civil society, academia, and other stakeholders, investigate, document, and publish incidents and practices suspected to fall into the ambit of foreign influence on local laws and practices related to digital rights and democratic governance.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
+256 414 289 502
programmes@cipesa.org
@cipesaug facebook.com/cipesaug Linkedin/cipesa
www.cipesa.org