10 CASE STUDY: COMBATTING CYBER THREATS, DISINFORMATION, AND INTERNET SHUTDOWNS

Estelle Masse, Access Now
Marwa Fatafta, Access Now
Felicia Anthonio, Access Now
Verónica Arroyo, Access Now

ABSTRACT

The same digital technologies that can improve people's lives also can be used to restrict freedoms and, deliberately or inadvertently, widen inequalities and exclusion. The potential for harms and abuses include cyber-attacks, disinformation and hate speech on social media, digital identification systems that fail to protect personal data and exclude marginalised populations, and so-called smart cities where digital tools enable the surveillance of citizens. As the pace of digitalisation accelerates, human rights-based policies and frameworks are urgently needed to manage both the negative and positive outcomes.

Key messages

- Through Internet shutdowns, disinformation and mismanaged digital ID programmes, many governments restrict human rights and fundamental freedoms. Nascent smart cities programmes are putting safety, privacy and public budgets at risk.
- Developing countries lag in cybersecurity capacity and enforcement, lacking the resources, technological know-how and ecosystems to effectively mitigate risks and respond to cybercrimes.
- Development co-operation actors should engage with civil society to evaluate the impact of digital technologies and tools and better assess community needs and mitigate risks.

Digital transformation provides a range of innovative and powerful tools that governments can deploy to improve public services and the lives of their citizens and, alternatively, to curtail free speech and conduct mass surveillance. Internet shutdowns have been on the rise for a decade, occurring even amid the COVID-19 pandemic when so much of the world's economic and social life was forced on line. By the same token, the same social media platforms that enable communication and community also host hate speech and disinformation. Digital identification (ID) programmes that promise more efficient public service delivery can also expose personal data to misuse and exclude populations without proper safeguards in place. Access Now monitors the uses of digital technology and calls out abuses and potential risks to governments, companies and civil society.

Internet shutdowns and free speech

Governments sometimes impose Internet shutdowns during critical moments, violating rights with a devastating impact on people's lives (Google, 2021[1]). In 2020, there were at least 155 documented Internet shutdown incidents in 29 countries even as billions of people turned to the Internet for school, work and communication during the COVID-19 crisis (Taye, 2021[2]). In the first five months of 2021, at least 50 Internet shutdowns were recorded in 21 countries. The longest on record started in November 2020 in Ethiopia's Tigray region, where war has raged for the past year, and has hampered humanitarian aid, disrupted businesses, and prevented journalists and human rights groups from uncovering abuses (Access Now, 2021[3]).

Governments and non-state actors also have used social media to spread disinformation, propaganda or hate, interfere with elections, and abuse private data.

Disinformation and hate speech

Governments and non-state actors also have used social media to spread disinformation, propaganda or hate, interfere with elections, and abuse private data (Access Now, 2021[4]) and to enforce discriminatory laws. In these cases, though tech tools became an enabler of harm, companies often failed to anticipate, mitigate or respond to the risks. Internal Facebook documents about the company's operations "paint a grim picture" (Garfield, 2021[5]). For instance, the Facebook Papers reveal that employees repeatedly criticised the company's failure to limit posts inciting violence in Ethiopia (Access Now, 2021[6]) and warned managers about "problematic actors" spreading inflammatory content (Mackintosh, 2021[7]). Despite huge deployment in the Middle East and Africa, for instance, most tech companies fail to engage civil society in the region or hire content reviewers and employees who understand local languages, context and nuances (Gani, 2021[8]).

Digital identification and exclusion

In recent years, governments and development actors have focused on developing ID systems. The World Bank Group, through its Identification for Development, or ID4D, initiative[1] has mobilised more than USD 1 billion to support civil registration and related projects in over 45 countries (World Bank, 2019[9]). But in many countries, digital ID systems have been developed without first considering the impacts on equality, privacy and security (Aggarwal and Chima, 2021[10]). This raises two questions: First, whether access to public services should depend on having government ID; and second, whether identification systems should be only digital.

In countries with digital ID systems, citizens may have to register for online identification to claim benefits or access essential services such as health, education and voting. These requirements do not always result in better service. In some cases, digital ID programmes simply move poor-quality services on line. They also can exclude individuals and entire communities. In India, for example, the digital Aadhaar card is often required to access vaccines and health centres have turned people away even when they have other official forms of identification (Chakravarti, 2021[11]). Such systems do not account for the digital divide in access to electricity and Internet access (Chandran, 2021[12]). Nor do they consider differences in access to electronic devices, digital literacy, or structural discrimination and inequality (Renaldi, 2021[13]).

In addition, while governments collect a trove of personal data, safeguards to protect these data from fraud or theft are sometimes missing and data breaches have occurred. Kenya enacted comprehensive data protection legislation in 2019 (Access Now, 2021[14]), and Ethiopia, India and Uganda are considering proposed data protection measures alongside the introduction of digital ID programmes. Done right, these safeguards protect people's rights beyond securing their information. But the legislation in these countries is either stalled or difficult to enforce. Other countries rushed the adoption of data protection as a box-ticking exercise when the need is for human rights-centred approaches aligned to principles of transparency, good governance and public consultation.

The #WhyID coalition,[2] led by Access Now, provides governments with a set of questions about the objectives, needs and benefits of digital ID programmes to be considered before they are implemented. Access Now also publishes a do's and don'ts guide for lawmakers to assist them in developing data protection laws that will protect and empower people.[3]

Cybercrime and surveillance

Positive outcomes from digitalisation require online security; safety and privacy; and a trusted, resilient cyberspace. The International Telecommunication Union has warned of a growing cyber capacity gap, with least developed countries especially lacking the resources, technological know-how and cybersecurity ecosystem to effectively mitigate the growing cyber risks and prepare for "opportunistic actors that [take] advantage of our desire for information" (ITU, 2020[15]). Box 10.1 outlines the knowledge and infrastructure gaps in Africa and initiatives to help governments build cyber capacity.

The privacy and human rights impact of the spread and commercialisation of digital technologies are also a challenge. For instance, digital technologies meant to make cities safer can erode freedoms. In smart cities, people interact with sensors, cameras, biometric tech and other tools that can lead to increased surveillance. Governments largely do not address the privacy and human rights impact of these technologies. Many of the smart cities in Africa that were billed as the solution to poverty and urban crime are considered failures (Baraka, 2021[24]). In some countries, social and welfare spending

BOX 10.1. NEW INITIATIVES AIM TO IMPROVE CYBERSECURITY IN AFRICA

PROVIDED BY AFRICA TEAM, GLOBAL FORUM ON CYBER EXPERTISE

While African countries have made progress in their commitments to respond to cybersecurity threats, challenges remain to building a secure and resilient cyberspace. The International Telecommunication Union's latest Global Cybersecurity Index suggests that many African countries need to reach more robust cybersecurity levels and notes that the COVID-19 crisis demonstrates that collective action problems such as health security and cybersecurity require a multidisciplinary and comprehensive approach (ITU, 2020[15]). The African Union's 2020-30 Digital Transformation Strategy for Africa also highlights the need for a greater capacity to detect and mitigate cyberattacks (African Union, 2020[16]).

Governments and international bodies should collaborate to promote cybersecurity in Africa. Development co-operation actors are stepping up support for cybersecurity with a focus on capacity building:

- The World Bank Global Cybersecurity Multi-Donor Trust Fund provides cybersecurity assessment and comprehensive cybersecurity capacity development (World Bank, 2021[17]). In collaboration with INTERPOL, the United Kingdom is investing GBP 22 million to establish new cyber operation hubs in Ghana, Kenya, Nigeria and Rwanda to facilitate joint cybercrime operations (UK Government, 2021[18]).
- The African Development Bank has contributed USD 2 million to establish the African Cybersecurity Resource Center to deliver cybersecurity services and information exchange across Africa (African Development Bank, 2021[19]). The Africa Cyber Capacity Building Coordination Committee aims to provide oversight on specific projects and develop new projects for the region (African Union Development Agency, 2021[20]).
- A programme of the Global Forum on Cyber Expertise and the African Union will build a community of cyber experts from the different African countries, identify national cyber capacity gaps, prioritise and communicate cyber capacity needs, and co-ordinate existing and emerging cyber capacity-building efforts in Africa (Global Forum on Cyber Expertise, 2021[21]).

Currently, cybersecurity legislation, policies and standards have yet to be developed in Africa. Only two countries have computer emergency response teams and computer security incident response teams that are fully equipped and operational. Only 11 institutions on the continent offer cybersecurity training (Keystone Masterstudy, 2021[22]). Where cybersecurity laws exist, they have sometimes produced negative outcomes. Legislation and regulations affecting digital service users in Burundi, the Democratic Republic of the Congo, the United Republic of Tanzania, Uganda and Zambia have undermined producer and consumer trust and restricted human rights (CIPSEA, 2019[23]).

Tightening cybersecurity must not damage Internet openness or user trust. Protocols or standards on cybersecurity also should be developed in consultation with different stakeholders and international agreements on related areas such as electronic payments and data protection should take cybersecurity into account. The 2014 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) incorporates such a cross-cutting approach. The Convention is yet to enter into force.

suffered as resources went to pursue investment for these projects. Moreover, the tech systems meant to fix societal issues have proved ineffective. In Nairobi, crime fell by 46% in the first year after a Huawei-built surveillance system was installed in 2014, rose by 13% and then by an additional 50% in 2016 and 2017 (Baraka, 2021[24]).

REFERENCES

Access Now (2021), *Data Protection in Kenya: How is This Right Protected?*, Access Now, Brooklyn, NY, https://www.accessnow.org/cms/assets/uploads/2021/10/Data-Protection-in-Kenya.pdf (accessed on 8 November 2021). [14]

Access Now (2021), "LGBTQI communities: Proud and secure online", web page, https://www.accessnow.org/lgbtqi-communities-proud-and-secure-online (accessed on 8 November 2021). [4]

Access Now (2021), *Open letter to Facebook on violence-inciting speech: act now to protect Ethiopians*, https://www.accessnow.org/open-letter-to-facebook-protect-ethiopians/ (accessed on 8 November 2021). [6]

Access Now (2021), "What's happening in Tigray? Internet shutdowns avert accountability", web page, https://www.accessnow.org/tigray-internet-shutdowns (accessed on 8 November 2021). [3]

African Development Bank (2021), "The African Development Bank extends a grant of $2 million to strengthen cybersecurity and boost financial inclusion in Africa", press release, African Development Bank, https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-extends-grant-2-million-strengthen-cybersecurity-and-boost-financial-inclusion-africa-42526 (accessed on 10 November 2021). [19]

African Union (2020), *The Digital Transformation Strategy for Africa (2020-2030)*, African Union, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf. [16]

African Union Development Agency (2021), "Africa Cyber Capacity Building", African Union Development Agency, https://www.nepad.org/news/africa-cyber-capacity-building (accessed on 10 November 2021). [20]

Aggarwal, N. and R. Chima (2021), "Privacy for sale: India is pushing for more data exploitation, not personal data protection", *Access Now Blog*, https://www.accessnow.org/india-personal-data-protection (accessed on 8 November 2021). [10]

Baraka, C. (2021), "The failed promise of Kenya's smart city", Rest of World, New York, NY, https://restofworld.org/2021/the-failed-promise-of-kenyas-smart-city (accessed on 8 November 2021). [24]

Chakravarti, A. (2021), "For Covid-19 vaccine Aadhaar is mandatory even if registration on CoWin done with other ID. Sort of.", India Today, https://www.indiatoday.in/technology/news/story/for-covid-19-vaccine-aadhaar-is-mandatory-even-if-registration-on-cowin-done-with-other-id-sort-of-1805290-2021-05-21 (accessed on 8 November 2021). [11]

Chandran, R. (2021), "India's digital IDs for land could exclude poor, indigenous communities", Reuters, https://www.reuters.com/article/india-landrights-digital-idUSL8N2LT0E6 (accessed on 8 November 2021). [12]

CIPSEA (2019), *Digital Rights in Africa: Challenges and Policy Options*, Collaboration on International ICT Policy for East and Southern Africa, Kampala, https://cipesa.org/?wpfb_dl=287 (accessed on 12 November 2021). [23]

Gani, A. (2021), "Facebook's policing of vitriol is even more lackluster outside the US, critics say", The Guardian, https://www.theguardian.com/technology/2021/oct/17/facebook-policing-vitriol-outside-us (accessed on 8 November 2021). [8]

Garfield, L. (26 October 2021), "What you need to know about the Facebook Papers", *Access Now Blog*, https://www.accessnow.org/facebook-papers-what-you-need-to-know (accessed on 8 November 2021). [5]

Global Forum on Cyber Expertise (2021), "AUC-GFCE Collaboration: "Enabling African countries to identify and address their cyber capacity needs"", Global Forum on Cyber Expertise, https://thegfce.org/auc-gfce-collaboration-enabling-african-countries-to-identify-and-address-their-cyber-capacity-needs (accessed on 10 November 2021). [21]

Google (2021), "The Current: The Internet shutdowns issue", *Jigsaw* 4, https://jigsaw.google.com/the-current/shutdown (accessed on 8 November 2021). [1]

ITU (2020), *Global Cybersecurity Index 2020*, International Telecommunication Union, Geneva, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. [15]

Keystone Masterstudy (2021), "Masters programs in cybersecurity in Africa 2022", web page, https://www.masterstudies.com/Masters-Degree/Cyber-Security/Africa. [22]

Mackintosh, E. (2021), "Facebook knew it was being used to incite violence in Ethiopia. It did little to stop the spread, documents show", CNN Business, https://edition.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html (accessed on 8 November 2021). [7]

Renaldi, A. (2021), "Indonesia's invisible people face discrimination, and sometimes death, by database", Rest of World, https://restofworld.org/2021/indonesias-invisible-people-face-discrimination-and-sometimes-death-by-database (accessed on 8 November 2021). [13]

Taye, B. (2021), *Shattered Dreams and Lost Opportunities: A Year in the Fight to #KeepItOn*, Access Now, Brooklyn, NY, https://www.accessnow.org/cms/assets/uploads/2021/03/KeepItOn-report-on-the-2020-data_Mar-2021_3.pdf. [2]

UK Government (2021), "UK pledges £22 million to support cyber capacity building in vulnerable countries", press release, UK Government, London, https://www.gov.uk/government/news/uk-pledges-22m-to-support-cyber-capacity-building-in-vulnerable-countries (accessed on 10 November 2021). [18]

World Bank (2021), "Cybersecurity Multi-Donor Trust Fund", web page, https://www.worldbank.org/en/programs/cybersecurity-trust-fund. [17]

World Bank (2019), "Inclusive and trusted digital ID can unlock opportunities for the world's most vulnerable", World Bank, Washington, DC, https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable (accessed on 8 November 2021). [9]

NOTES

1. For more information on the initiative, see: https://id4d.worldbank.org.
2. For more information on the coalition, see: https://www.accessnow.org/whyid.
3. For more information, see: https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf.

From:

Development Co-operation Report 2021

Shaping a Just Digital Transformation

Access the complete publication at:
https://doi.org/10.1787/ce08832f-en

Please cite this chapter as:

Masse, Estelle*, et al.* (2021), "Case study: Combatting cyber threats, disinformation, and Internet shutdowns", in OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/c65b2612-en