USAID
FROM THE AMERICAN PEOPLE

Digital Threats to Democracy in the Economic Growth Sector



Digital threats to democracy are a growing topic of conversation among those in the Democracy, Human Rights and Governance (DRG) sector. The reality is that digital threats affect all USAID sectors, including economic growth, agriculture, education, and global health. As noted in USAID's Digital Strategy, the increased use of digital tools and technology has brought many opportunities for improved outcomes in USAID partner countries. However, technology also provides an avenue for undemocratic actors to manipulate information, exploit private data, surveil public space, and impinge upon human rights. Building on the findings of the Bureau for Africa's 2021 Democratizing Digital Landscape Assessment, USAID has identified an important need and opportunity to further integrate awareness of digital threats to democracy into its programming. A 2022 digital development portfolio mapping of USAID digital development efforts showed that safeguards to protect privacy, human rights, and democratic freedoms are underrepresented and underreported in USAID-funded projects. This underscores the importance of countering and mitigating digital threats to democracy across USAID programming in sub-Saharan Africa is critical. This document looks into the intersection of digital threats to democracy and the education sector for a USAID audience with an Africa focus. It offers recommendations for strategically raising awareness of digital threats to democracy and incorporating these considerations into programming, and explores key trends in digital threats to democracy across the economic growth sector.

How USAID Can Mitigate Digital Threats to Democracy In Its Economic Growth Programming

Mobile technologies and associated services accounted for $5.2 trillion of economic value added in 2022, or five percent of global gross domestic product, and was responsible for 28 million jobs around the globe, according to GSMA.[1] The benefits of digital tools and technologies in low- and middle income countries are clear. They increase economic productivity, improve efficiency, lower transaction costs, and promote innovation.[2] USAID's 2021 Economic Growth Policy centers the role of digital tools in economic growth by stating that "Interventions that strengthen market-driven digital ecosystems and draw people into the digital arena are essential for economic growth and human development…"[3] Identifying and mitigating the potential for digital threats to democracy across USAID's economic growth portfolio supports inclusive, resilient, and sustainable economic growth while promoting open, inclusive, and secure digital ecosystems in USAID partner countries.

1 The Mobile Economy 2023 | GSMA

2 World Development Report 2016: Digital Dividends | World Bank

3 Economic Growth Policy | United States Agency for International Development

USAID can play an important role in fighting and mitigating digital threats to democracy through its economic growth portfolio. The box below highlights key questions to consider during program design. This is followed by specific recommendations for USAID staff based in Washington and USAID Mission staff and implementing partners aiming to address these issues in their economic growth and digital economy programming.

Ensuring the use of rights-respecting technologies in USAID economic growth programming

Digital tools can accelerate development outcomes in USAID partner countries, but they can also pose digital threats to democracy. These threats may not be immediately clear. In considering the range of potential digital threats to democracy in the short- and long-term stemming from digital interventions in economic growth programming (e.g. digital tools, technologies, policies, processes, systems, or other digital ecosystem- oriented interventions), ask the following questions considering three distinct scenarios:

1. impact under the current government,
2. impact if the current government begins or accelerates the process of democratic backsliding, and
3. impact under a new, more authoritarian government.

Questions for consideration:

- How can this intervention promote or be affected by **digital surveillance**?
- How can this intervention promote or be affected by **misinformation, disinformation, or malinformation**?
- How can this intervention promote or be affected by **online censorship**?
- How can this intervention promote or be affected by **internet shutdowns**?
- How can this intervention promote or be affected by **targeted online persecution**?
- How can this intervention promote or be affected by **offline persecution for online behavior**?
- How can this intervention potentially expose individuals to t**argeted harassment or legal issues** based on their gender, identity, or perceived affiliation with a group such as LGBTQI+?
- How can this intervention be positively or negatively affected by **data localization**?
- What are **other potential misuses of this intervention**?

Recommendations for USAID/Washington staff

These recommendations address how USAID/Washington staff can raise awareness of digital threats to democracy within their sectors and USAID portfolios – in this case, economic growth.

Internal-facing

Develop guidance for USAID staff and implementing partners on how to apply the *Donor Principles for Human Rights in the Digital Age* to programming in the economic growth sector. This will help ensure that USAID does not fund non-rights-respecting technologies.

Design and provide practical, hands-on training to USAID staff and implementing partners about:

- The risk of digital threats to democracy in the economic growth sector, with a focus on concrete strategies to identify and mitigate potential digital rights abuses in their programming.
- Assessing cybersecurity risks in their programming and integrating adequate cybersecurity protections into their work, which can prevent or mitigate the effects of digital threats to democracy.
- Developing and disseminating practical tools to aid in determining vulnerabilities and deploying effective countermeasures.[4]

4 Available USAID resources include Democratizing Digital Video and Facilitator's Guide; Digital Literacy Sectoral Briefers; Cybersecurity Sectoral Briefers; Digital Government Sectoral Briefers; Principles for Digital Development Training: Economic Growth (USAID internal)

Fund targeted research to identify how digital threats to democracy manifest in the digital economy, such as data on economic losses due to internet shutdowns or how "brain drain" that can result in the wake of digital rights abuses affects the startup sector.

Design and test evaluation methods to measure the impact of digital threats to democracy and associated mitigation strategies in the economic growth sector, with the objective of developing indicators to incorporate into activity and intervention design.

Gather evidence from USAID-funded programs on how to mitigate the impact of digital rights abuses on economic growth, in order to replicate or adapt these methods in new programming.

External-facing

Facilitate the development of codes of conduct and software development standards for the design and use of digital services for the digital economy based on the Principles for Digital Development and the principle of Do No Harm.

Collaborate with other U.S. Government agencies that work to strengthen the strategic and economic partnership between the U.S. and Africa to **minimize the export of non-rights-respecting technologies or dual use technologies[5] to USAID partner countries**,[6] aligned with the Export Controls and Human Rights Initiative.

Recommendations for USAID Mission staff and implementing partners at the country level

These recommendations address how USAID Mission staff can raise awareness of and counter digital threats to democracy in their economic growth portfolios at the country level.

Track rapid shifts in the local digital ecosystem or digital economy that may indicate emerging digital threats to democracy, with a particular focus on digital policies that affect businesses. Rapid changes in digital policies or sudden crackdowns can create uncertainty, which can discourage long-term investments and hinder economic planning.

With national governments in USAID partner countries:

Align regulatory frameworks for the digital economy with democratic values.

- Provide technical assistance (TA) on topics including data protection, privacy, and cybersecurity, and collaborate with in-country legal experts to localize appropriate model legislation and adapt best practices to the local context. This aligns with USAID's Economic Growth Policy, which emphasizes that governments also need to avoid non-transparent, counterproductive restrictions on flows of data, because such restrictions can have the effects of impairing trade and foreign investment, making local digital ecosystems less secure, and harming the economic prospects for small and medium enterprises (SMEs).[7]

5 Technologies that can facilitate digital rights abuses, but that also can be used for other legitimate purposes. Examples include "smart cities" technology, which governments can use for legitimate public safety purposes if appropriate safeguards are in place, but can also cause digital rights abuses.

6 Digitized Autocracy Literature Review: Final Report | NORC at the University of Chicago

7 Economic Growth Policy | United States Agency for International Development

- Engage a broad cross-section of digital economy and digital rights stakeholders such as startups, activists, consumers, foreign and local investors, civil society organizations (CSOs), consumer protection agencies, and micro, small, and medium enterprises (MSMEs) in policy-making processes related to digital technology.[8]
- Encourage the development of local, national, and regional economic growth laws, policies, and regulations aligned to international norms and standards in USAID partner countries that 1) reduce barriers to digital transactions, trade, e-commerce, and market access and 2) promote greater inclusion and equity within the digital economy.
- Promote regulatory alignment across USAID partner countries through mechanisms like the Budapest Convention (a rights-respecting anti-cybercrime framework with 68 parties, including the United States), further facilitating their integration into the global digital economy.
- Provide TA to governments on safeguarding digital public infrastructure[9] with economic growth applications, such as enhancing supervisory technologies for digital financial services (DFS).[10]

Work with regulatory authorities to enact effective import and export controls on non-rights-respecting technologies and dual use technologies. This includes preventing or carefully regulating their importation from other countries, as well as developing appropriate controls for the export of any relevant domestic technology products.

Sign onto voluntary initiatives that counter digital threats to democracy in the economic growth sector, such as the Export Controls and Human Rights Initiative or the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. Provide TA to effectively implement provisions of these initiatives at the country level.

With private sector stakeholders:

Upskill technology companies on developing rights-respecting digital tools and technologies.

- Provide training, coaching, and TA to software engineers and developers to identify, account for, and effectively tackle potential digital threats to democracy during the product development process.[11] This includes countering mis- and disinformation, effectively implementing national policies and regulations on data and technology (e.g., cost implications of centralized databases, data protection/cybersecurity applications and platforms, etc.), increasing cyber hygiene and access to digital safety resources, and integrating and enforcing consumer protection related to digital rights.
- Work with technology executives and software developers to prioritize cybersecurity by design and privacy by design principles when developing new digital tools, such as minimizing the amount of personally identifiable information that DFS, banking, and other related digital tools collect about their customers.
- Provide TA to embed digital rights within company processes by 1) ensuring that their management conduct due diligence to recognize and account for the impact of their products on digital threats to democracy, 2) publicly sharing any policies that could impact users' digital rights, such as data sharing with the government, and 3) creating a formal redress process for anyone who believes their rights were violated by using the digital tool.[12]
- Promote the adoption of the United Nations Guiding Principles on Business and Human Rights among companies who create digital tools that could be used to infringe upon others' digital rights.[13]

---

8 Digital Transformation and the Futures of Civic Space to 2030 | Organization for Economic Cooperation and Development

9 The Center for Strategic & International Studies (CSIS) defines digital public infrastructure as "the network of digital building blocks that are needed to deliver public services across sectors" in Advancing Digital Transformation and Digital Public Infrastructure.

10 The promise of DPI won't be realized with good design alone. Safeguards are key. | Digital Impact Alliance (DIAL)

11 Digital Transformation and the Futures of Civic Space to 2030 | Organization for Economic Cooperation and Development

12 Digital Transformation and the Futures of Civic Space to 2030 | Organization for Economic Cooperation and Development

13 Digitized Autocracy Literature Review: Final Report | NORC at the University of Chicago

Work with local partners to build MSMEs' awareness of digital threats to democracy, like mis- and disinformation, through large scale communications campaigns and existing programming for MSMEs, such as trainings.

Build the capacity of MSMEs to integrate and enforce safeguards against digital rights abuses in their product development processes and in internal company policies.

Work with financial institutions to develop new loan or insurance products that allow businesses to invest in their own cybersecurity. This can mitigate potential digital rights abuses.

With civil society and consumers:

Bring together and facilitate linkages between the private sector, including multinational technology companies, and civil society in countering digital threats to democracy. This will help private sector stakeholders to develop, implement, and roll-out rights-respecting technologies and improve activists' knowledge of private sector pain points so they can develop tailored strategies to counter digital rights abuses.

Provide TA or capacity-building support to consumer advocacy groups. This can play an important role in identifying and advocating against specific instances of digital rights violations in the digital economy and can influence industry norms to minimize digital threats to democracy.

Increase consumer knowledge and awareness of digital threats to democracy across the digital economy. This may include building the capacity of individual consumers to recognize and minimize their use of non-rights-respecting digital tools through large scale communications campaigns or as part of larger trainings.

Key Trends in Digital Threats to Democracy Across the Economic Growth Sector

Digital threats to democracy can have a profound impact on economic growth in USAID partner countries by reducing competitiveness, disincentivizing investment, discouraging trade opportunities, and undermining innovation. Current trends around the globe and in sub-Saharan Africa include:

- **Internet shutdowns and censorship on digital platforms are already affecting the economies of USAID partner countries, causing significant financial losses**. Technology companies are banning the accounts of businesses and entrepreneurs, while governments are arresting business executives for their online activities, weaponizing e-commerce data to impose unfair taxes or fines on individual businesses, and censoring business leaders online. In 2022, the livestream of well-known Chinese e-commerce entrepreneur Li Jiaqi (or Austin Li) was cut immediately after his assistant held up a dessert that resembled a military tank. After years of hosting daily livestreams to sell consumer products and goods, Li did not livestream for three months after this incident.[14] Internet shutdowns similarly have dire implications for the economy. In 2022, internet shutdowns in sub-Saharan Africa cost the economy USD 295 million. Ethiopia alone accounted for USD 180 million of those losses.[15] A 2019 paper calculated that "fake news" costs the world economy USD 78 billion annually,[16] while the Lagos Chamber of Commerce and Industry estimated that Nigeria's seven-month ban on Twitter in 2021-2022 cost the country an

14 The Return of the Lipstick King | Rest of World

15 Government Internet Shutdowns Cost $24.6 Billion in 2022 | Top 10 VPN

16 Online fake news is costing us $78 billion globally each year | ZDNET

estimated USD 26.1 billion.[17] These examples indicate that digital threats to democracy are not an abstract issue for the economies of USAID partner countries and that they are negatively affecting economic outcomes in low- and middle-income countries.

- **Sweeping yet vague laws on data protection, data localization, cybersecurity, and cybercrime in USAID partner countries can disincentivize economic activity**. Well-written laws can enhance privacy and cybersecurity protections for citizens, while poorly written or overly broad laws can facilitate digital rights violations. Tanzania's 2015 Cybercrime Law does not uphold the right to due process because it allows Tanzania's police to conduct digital surveillance operations without judicial approval.[18] Vietnam's 2018 cybersecurity law mandates that major social media platforms remove content that the Government of Vietnam (GoV) considers "toxic" or offensive within one day and that they store their data locally so they can share it with the GoV upon request.[19] In this way, digital threats to democracy erode the confidence of local and foreign companies—including innovative startups emerging from the local digital ecosystem—by signaling weak rule of law and an unfavorable business environment. The Information Technology and Innovation Foundation estimates that a "1-point increase in a nation's data restrictiveness cuts its gross trade output 7 percent, slows its productivity 2.9 percent, and hikes downstream prices 1.5 percent over five years."[20] These examples underscore the importance of carefully crafting rights-respecting laws and regulations governing the intersection of technology and economic growth appropriate for a range of private sector stakeholders.
- **MSMEs and individual consumers are particularly vulnerable to mis- and disinformation and digitally-enabled targeted persecution, which can affect long-term economic outcomes**. Recent research with MSMEs in Kenya, India, and Cambodia showed that misinformation (such as gossip, fake reviews, and doctored photos) was the second most frequently reported harm associated with online tools and platforms.[21] Misinformation can also cause major businesses to fail. In 2016, Chase Bank in Kenya went bankrupt because widely circulated WhatsApp messages and tweets about alleged fraud caused a bank run, with depositors pulling out their funds.[22] Consumers may choose not to engage in the digital economy because of potential digitally-enabled targeted persecution. Aggressive debt collection practices among some DFS providers in Nigeria and Kenya can include accessing the contact lists of customers who have defaulted. These companies often aggressively pursue repayment by messaging multiple people on these contact lists stating that a particular individual owes money.[23] These practices may disincentivize consumers from using DFS, with broader implications for economic development. It is critical for USAID staff and implementing partners to address the real or perceived impact of digital threats to democracy on MSMEs and individual consumers.
- **Tight government restrictions, surveillance, or censorship of digital activities may cause "brain drain," leading to an underdeveloped innovation and startup sector within the local digital ecosystem**. Highly educated and talented individuals may choose to leave a country where their digital rights are restricted. The MIT Technology Review estimated that one-third of the employees of Yandex—a major Russian technology company—left Russia within two months of its 2022 invasion of Ukraine, following years of increasingly tighter state control

17 Nigeria lost $26bn to Twitter ban, businesses say | African Business

18 Tanzania: Cybercrime Act 2015 Legal Analysis | Article 19

19 Freedom on the Net 2019: Vietnam | Freedom House

20 How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them | Information Technology & Innovation Foundation

21 No Reward Without Risk: Addressing the Economic Impacts of Misinformation and Other Digital Harms on MSMEs | DAI

22 Online disinformation and the African firm | Nanyang Technological University

23 Nigerians blackmailed by loan apps are plotting revenge in Facebook groups | Rest of World; This lending app publicly shames you when you're late on loan payment | Rest of World

over Yandex and widespread digital rights violations across Russia.[24] This exodus of skilled professionals can weaken the economy's ability to innovate, which can affect the entire economy with a disproportionate impact on the local startup and innovation sectors. This finding indicates that USAID's workforce development programming and support to local startup sectors must consider potential digital rights violations as a driver of "brain drain."

- **While some private companies sell technology products that enable human rights violations, others are developing programs to counter digital threats to democracy**. Chinese companies are major exporters of digital tools for surveillance technology. As of 2019, China had sent surveillance technology to more than 60 countries,[25] and at least 12 Chinese companies were involved in 75 "smart cities" or "public safety solutions" efforts and in over 200 data centers globally.[26] This phenomenon is not exclusive to autocratic states. Israeli companies are noted exporters of digital surveillance technologies, like the NSO Group's Pegasus spyware, which has been discovered on the phones of prominent activists or opposition members in at least 15 countries.[27] Other companies are fighting back against technology-facilitated human rights abuses. Microsoft's Defending Democracy Program collaborated with civil society groups, academics, and national governments to "protect campaigns from hacking; increase political advertising transparency online; explore technological solutions to preserve and protect electoral processes; and defend against disinformation campaigns and cyberattacks."[28] The private sector's dual role in spreading digital tools that violate human rights, while simultaneously countering technology's negative impacts on democracy, suggests that USAID will need to carefully choose its partners for economic growth programming.

These trends highlight the growing need for USAID and implementing partners to consciously integrate safeguarding into economic growth programming involving digital tools and technology. To learn about recommendations and trends in digital threats to democracy for other USAID sectors, please refer to the following (to be linked):

- Digital Threats to Democracy - Education
- Digital Threats to Democracy - Health
- Digital Threats to Democracy - Agriculture

Please contact USAID/AFR/CPG afrdigital@usaid.gov for more information.

24 How Russia Killed Its Technology Industry | MIT Technology Review

25 China's Role in Global Digital Repression | Global Policy

26 China's Role in Global Digital Repression | Global Policy

27 Digitized Autocracy Literature Review: Final Report | NORC at the University of Chicago

28 Digital Transformation and the Futures of Civic Space to 2030 | Organization for Economic Cooperation and Development