July 2024

Digital Threats to Elections

Learning From What Has Worked in Africa

Study by Abi Watson and Fennet Habte

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

stabilization lab

Table of Contents

Executive Summary

Digital threats to elections are rapidly evolving around the world, threatening to undermine democratic institutions and spark electoral violence. International, national and local organizations seek to mitigate these threats, but it is not easy to tell which efforts have worked. What is more, limited time and funding often leaves little room to learn from past elections. To address this, our team spent the past year engaging with over 100 experts and practitioners from civil society organizations (CSOs), governments, international bodies, and election assistance funders across Africa. This project, inspired by German and UNDP efforts to revamp funding structures for democratic elections in Africa, aims to glean insights from successful case examples from across the continent to enhance donor and implementer strategies against digital election threats – both in Africa and around the world.

Our research identified four key "building blocks for success" present in programming that managed to mitigate digital threats to elections on the African continent. Recognizing that there is not an endless pot of funding for such activities, we explored how different levels of investment (high, medium and low) can contribute to each of these building blocks.

Building Block One: Understanding the "Digital Threat Landscape

In many cases, we found that funders rely on faulty or uninformed assumptions – often drawn from headlines – about the most pressing electoral issues or the most useful contributions they could make, which resulted in ineffective or even counterproductive interventions. More successful efforts have used baseline surveys, iterative learning and post-programming reviews to target real needs and follow effective theories of change.

With high investment:
Baseline surveys, iterative learning & endline assessments

With medium investment:
Learning as we go (and planning for it)

With minimal investment:
Asking whether programming worked

Building Block Two: Varied Actors for Varied Digital Threats

When working alone, organizations will always struggle to respond to the multiple issues entailed by digital threats at the scale required. More successful efforts have brought together a variety of stakeholders (through coalitions, strategic coordination and facilitated networking) and developed multi-pronged solutions, which tackled a diverse range of threats by sharing information and coordinating action.

With high investment:
Investing in coalitions

With medium investment:
Supporting strategic coordination

With minimal investment:
Facilitating networking

Building Block Three: Taking An Institutional Approach to Digital Threats

Training that focuses on individual-level skills for a small cohort – for instance journalists, activists or representatives of electoral management bodies – will have little impact if the trainees' organizations are unable to absorb the improvements brought back to them. More successful efforts bolstered organizations as a whole by co-designing projects, implementing organization-wide trainings and filling core institutional capacity gaps (not just funding more projects), which are more sustainable models over the long term.

With high investment:
Co-design localized election work

With medium investment:
Work on gaps in institutions

With minimal investment:
Fund core capacity, not just another program

Building Block Four: Hybrid Solutions for Hybrid Problems

By just focusing on "digital fixes," donors and implementers miss that digital threats also emerge from and extend to offline spaces. This creates the risk of developing strategies that are poor matches for their context. More successful efforts have sought to understand the actual "digital need," as well as the capacity of CSOs and their target audiences to actually use technology. In many cases this has resulted in more appropriate (and often much lower-tech) solutions to pressing threats.

With high investment:
Tailoring to the tech need

With medium investment:
Assess the capacity to use tech

With minimal investment:
Consider lower tech solutions

The resourceful approaches showcased by the organizations we spoke to not only provide valuable lessons for tackling digital threats in Africa, but also offer insights that apply wherever implementers and funders want to develop programs to effectively safeguard elections from digital threats.

Introduction

Those seeking to support good governance in Africa have long looked to successful elections as a marker of progress. Free and fair elections are a cornerstone of democracy – and a serious threat to anyone whose claim to political power would not survive a true popular vote. Elections are therefore often a target for fraud and a pretext for violence. Alongside traditional offline techniques such as ballot stuffing and vote buying, malign actors have added new digital options to their toolboxes for silencing dissent and influencing democratic political expression, such as increasingly affordable surveillance and hacking software.[1]

This report understands digital threats to elections as those emanating from the online space or responding to activities online. These threats include mis- and disinformation, internet shutdowns, restrictive cyber laws, hacking, and surveillance (see Glossary on pgs. 9–10). Digital threats have proliferated around the world, contributing to rising authoritarianism, eroding trust in elections and stoking pre- and post-electoral violence.

Arguably, the consequences of these threats are even greater in fragile democracies, many of which are in sub-Saharan Africa.[2] In countries where democratic norms are new or contested, actors seeking to bias election results not only focus on reducing votes for the other party but also often work to undermine trust in the electoral systems and electoral management bodies (EMBs) themselves.[3] These patterns repeat themselves around the world, but armed conflict and military coups in the Sahel and the Horn of Africa have brought the challenges to democracy on the continent into sharp focus.

According to Freedom House, freedom in Africa has declined for the tenth consecutive year, with only 7 percent of Africans now living in a "free country."[4] In 2023 alone, Access Now and the #KeepItOn coalition documented 17 internet shutdowns in nine African countries: Ethiopia (4), Senegal (4), Guinea (2), Tanzania (2), Gabon (1), Somaliland (1), and Uganda (1).[5] Many of these shutdowns occurred around elections, which continue to be characterized "by political violence, administrative irregularities, and distrust" in numerous countries across the continent.[6] In addition to shutdowns, fact-checkers have argued that the exponential spread of mis- and disinformation in many contexts pose "existential" dangers, with smear campaigns, widespread lies about rigged elections, and premature declarations of victory proving nearly impossible to stop.[7] All this is happening against the backdrop of social media companies dismantling already under-resourced content moderation and "trust and safety"

1 Adrian Shahbaz and Allie Funk, "Digital Election Interference," *Freedom House*, accessed April 5, 2023, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/digital-election-interference.

2 Freedom House, "Africa Marks a Decade of Decline in Freedom, with 2023 Being Marred by Electoral Violence and Civil Conflict," February 29, 2024, accessed May 18, 2024, https://freedomhouse.org/article/new-report-africa-marks-decade-decline-freedom-2023-being-marred-electoral-violence-and.

3 Fortune Agbele, "Disinformation and Voter Confidence During Kenya's 2022 Election," *Megatrends Afrika*, March 30, 2023, accessed June 6, 2024, https://www.megatrends-afrika.de/10.18449/2023MTA-PB14/.

4 Freedom House, "Africa Marks a Decade of Decline in Freedom," February 29, 2024.

5 Zach Rosson, Felicia Anthonio and Carolyn Tackett, "Shrinking Democracy, Growing Violence: Internet shutdowns in 2023," *Access Now*, May 2024, accessed May 15, 2024, https://www.accessnow.org/internet-shutdowns-2023/.

6 Freedom House, "Africa Marks a Decade of Decline in Freedom," February 29, 2024.

7 Abi Watson, "To Save Elections From Disinformation, Fact-Checking Is Only the First Response," *GPPi*, November 7, 2023, accessed June 6, 2024, https://gppi.net/2023/11/07/to-save-elections-from-disinformation-fact-checking-is-only-the-first-response.

teams on the African continent, thus closing avenues for timely support to take content down and mitigate these harms.[8]

In the background, the number of internet users in sub-Saharan Africa increased by 115 percent between 2016 and 2021.[9] Yet these newly connected users often have relatively low levels of digital literacy. This makes them especially vulnerable to, say, mis- and disinformation campaigns or hacking attempts. And as has been documented elsewhere,[10] in the past decade African governments and local authorities have begun adopting digital systems to manage public life and citizen–government relations (like digital IDs providing online access to public services or online electoral registers). In the absence of established data protection measures or accompanying public education programs, these same systems have been the subject of mis- and disinformation campaigns[11] and even hacking and cyber-attacks that endangered citizens data.[12]

Digital threats are inherently connected to (and shaped by) offline realities.

Digital threats are inherently connected to (and shaped by) offline realities. For instance, lies spread online spill into offline spaces as part of "the everyday communication of current affairs through discussions in marketplaces, places of worship, bars, and the like and through a range of non-conversational and visual practices such as songs, sermons, and graffiti."[13] Similarly, traditional media plays an important role in amplifying the spread of lies online: false stories may start on social media and circulate through messaging apps or word of mouth, then get picked up by television or radio shows, before turning up again online – thus reinforcing the same falsehoods and skewing reality even further. Those who are active online tend to also be influential actors in offline spaces, such as "political activists, journalists, social commentators and religious figures,"[14] wealthier individuals living in cities, and people in the diaspora. So even in countries where the number of direct internet users is low, online misinformation and disinformation can still spread through society because they reach people who are disproportionately able to shape national narratives for others.

Digital threats also exacerbate traditional offline harms and the marginalization that occurs during elections and throughout broader society. Women and gender minorities are often more vulnerable to online harms because of the power hierarchies present in society (as documented by the countless examples of women and LGBTQ individuals being uniquely targeted by online hate speech, lies and hacking). Likewise, journalists and civil society activists who call out authoritarian regimes – historically doing so offline, but increasingly also online – have long faced harassment, intimidation and arrest. The increased online surveillance of these same actors, including account and device hacks, are just additional tools to suppress critical voices.[15]

---

8 Billy Perrigo "New Lawsuit Accuses Facebook of Contributing to Deaths From Ethnic Violence in Ethiopia," *Time*, December 14, 2022, accessed June 6. 2024, https://time.com/6240993/facebook-meta-ethiopia-lawsuit/; digwatch, "Meta's content moderation in Africa is facing uncertainty," April 16, 2024, accessed June 6, 2024, https://dig.watch/updates/metas-content-moderation-in-africa-is-facing-uncertainty.

9 World Bank, "Digital Transformation Drives Development in Africa," January 18, 2024, accessed June 20, 2024, https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa.

10 ODI, "Digital Societies," accessed June 6, 2024, https://odi.org/en/topics/digitalisation/.

11 Fortune Agbele, "Disinformation and Voter Confidence During Kenya's 2022 Election," March 30, 2023.

12 Access Now, "Why ID?," accessed February 13, https://www.accessnow.org/campaign/whyid/.

13 Elena Gadjanova, Gabrielle Lynch and Ghadafi Saibu, "Misinformation Across Digital Divides: Theory And Evidence From Northern Ghana," *African Affairs* 121, no. 483 (April 2022): pp. 161–195, https://doi.org/10.1093/afraf/adac009.

14 Idayat Hassan and Jamie Hitchen, "How Hashtag Activism Moves Offline in The Gambia," *Democracy in Africa*, September 29, 2020, accessed June 6, 2024, http://democracyinafrica.org/hashtag-activism-gambia/.

15 Kate Bartlett, "Attacks, Harassment Threaten Media Across Africa," *Voice of America*, August 2, 2023, accessed January 23, 2024, https://www.voanews.com/a/attacks-harassment-threaten-media-across-africa-/7208922.html.

While the number of measures being used to mitigate the rise of digital threats is growing (see Glossary on pgs. 9–10), unfortunate funding limits have in many cases restricted efforts to learn from past elections. To start addressing this gap, our team has spent the last year interviewing, conducting surveys and running workshops with over 100 experts and practitioners from civil society organizations and coalitions, governments, international organizations, as well as funders of election assistance in Africa. While this work will have lessons for others beyond the continent, the project was inspired by German and UNDP efforts to revamp funding structures for supporting democratic elections in Africa.[16] Our aim was to identify lessons from good case examples for donors and implementers to improve their efforts against digital threats to elections on the continent. When surveying experts and practitioners about interventions that ably targeted the digital threat landscape in an upcoming election, we also looked to identify factors frequently linked to positive outcomes.

This research has resulted in four "building blocks for success," present in efforts that did mitigate some digital threats to elections in Africa:

Building Block One: Understanding the digital threat landscape: In many cases, we found funders relying on uninformed assumptions about the most pressing issue or most useful potential contribution, which resulted in ineffective or even counterproductive interventions. More successful efforts have used baseline surveys, iterative learning and post-programming reviews to target real needs and follow effective theories of change.

Building Block Two: Varied actors for varied digital threats: Single organizations or stakeholders will always struggle to tackle the multiple issues entailed by digital threats to elections – and to deliver the required responses at scale. More successful efforts have brought together a variety of stakeholders (through coalitions, strategic coordination and facilitated networking) and developed multi-pronged solutions, which relied on mutually shared information and coordinated action to tackle a diverse range of threats.

Building Block Three: Taking an institutional approach to digital threats: Training that focuses on individual-level skills (addressing a small cohort of journalists, activists or EMB representatives, for instance) will have little impact if the organizations they return to are unable to absorb improvements. More successful efforts addressed organizational gaps by (starting to pursue) co-designed projects, implementing organization-wide trainings and filling core institutional funding gaps – more sustainable long-term models than just funding another project.

Building Block Four: Hybrid solutions for hybrid problems: By just focusing on "digital fixes," donors and implementers miss that digital threats also extend offline. This creates the risk of developing strategies that are poor matches for their context. More successful efforts have sought to understand the actual "digital need" and gauge the technological capacity of CSOs and their target audiences. In many cases this has resulted in more appropriate (and often much lower-tech) solutions.

16 UNDP, "Germany and UNDP launch the Africa Election Fund to support electoral processes in Africa," January 25, 2023, accessed April 19, 2024, https://www.undp.org/africa/press-releases/germany-and-undp-launch-africa-election-fund-support-electoral-processes-africa.

Responding to the evident need for more practically minded learning, this report is oriented toward interventions at the programming level (i.e., specific projects funded to address a particular threat to a given election) rather than high-level discussions about how the international community should tackle digital threats. The politics behind these programming efforts, though, are also crucial. On the one hand, strategic-level buy-in from donors significantly impacts funding and coordination. Many organizations complained that budgets for their election work were cut as international donors changed their strategic priorities, or that they were forced to prioritize issues or intervention types they deemed to be less important simply because donors were funding them. International donors' buy-in also impacts the behavior of local politicians; interlocutors frequently noted that most political leaders are conscious of their international reputation, and that calls for fair and democratic elections from key figures can be very influential. (Kofi Annan, for instance, played a crucial role in convening 11 Nigerian presidential candidates to sign an inter-party agreement on non-violence and accept the 2015 election results.)

There are many cases where country elites and government actors are themselves a significant barrier to mitigating digital threats.

On the other hand, African governments' interest in mitigating digital threats will also inevitably bear on the effectiveness of programming. In fact, there are many cases where country elites and government actors are themselves a significant barrier to mitigating these threats, especially in countries that Freedom House rates as Partly Free, which are the "most likely to suffer internet freedom score declines surrounding elections."[17] Forbidden Stories, an international network of journalists, documented how incumbents and opposition parties in Africa (and elsewhere) have hired private companies to warp elections using a whole suite of digital threats.[18] As a staff member of a Kenyan CSO told us, "those who run the disinformation campaign get the top jobs in government when their candidate is elected."[19] Governments have also used disinformation to justify harsh laws and penalties against free speech, even extending to internet shutdowns.[20] The limits of programming in countries where governments are part of the problem is a perennial theme, and it certainly is no less true when it comes to mitigating digital threats. In the Sahel, where a recent wave of coups installed new military governments who have broken ties with France and the West more broadly, this problem is even more pronounced.[21]

Organizations in Africa have had to navigate the difficult politics in their countries, as well as within the countries and international organizations that fund them. This report focuses on what they have been able to do, at times against the odds. The next section will outline our methodology before considering distinct areas for change, and then exploring the main challenges and some ways in which CSOs, states and international organizations have sought to address them.

17 Adrian Shahbaz and Allie Funk, "Digital Election Interference," *Freedom House*, accessed April 5, 2023, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/digital-election-interference.

18 Forbidden Stories, "Story Killers: Inside the deadly disinformation-for-hire industry," accessed June 6, 2024, https://forbiddenstories.org/projects_posts/story-killers/.

19 Civil society representative, interview, Kenya, October 12, 2023; also see Stephanie Kirchgaessner, Manisha Ganguly, David Pegg, Carole Cadwalladr and Jason Burke, "Revealed: the hacking and disinformation team meddling in elections," The Guardian, February 15, 2023, accessed June 6, 2024, https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan.

20 Fennet Habte and Abi Watson, "Europe Needs a Nuanced Approach to Disinformation in African Elections," *Internationale Politik Quarterly*, March 5, 2024, accessed June 5, 2024, https://ip-quarterly.com/en/europe-needs-nuanced-approach-disinformation-african-elections.

21 Catherine Nzuki, "The Cost of Paternalism: Sahelian Countries Push Back on the West," *Center for Strategic & International Studies*, March 21, 2024, accessed June 6, 2024, https://www.csis.org/analysis/cost-paternalism-sahelian-countries-push-back-west.

Glossary of Digital Threats and Responses

The assortment of digital threats to elections is ever expanding. For the purposes of this report, we look at efforts aimed at mitigating the following threats:

misinformation

false information that is spread, regardless of any intent to mislead;

disinformation

information that is spread which is deliberately false, misleading or biased (e.g., purposefully taking something out of context);[22]

internet shutdowns

an intentional disruption of internet or electronic communications, rendering them inaccessible or unusable for a specific population or location, often to exert control over the flow of information;[23]

cyber laws

authoritarian laws and penalties that are introduced, purportedly to address the spread of false information, but with the actual aim "to silence dissenting voices, particularly during periods of unrest and elections";[24]

hacking and surveillance

incumbent regimes and external actors have targeted the phones, email and social media accounts of journalists, human rights defenders and opposition affiliates – in particular, through tools purchased from private companies, like the NSO Group's Pegasus spyware – to track dissenting voices and reduce their ability to operate.[25]

The range of responses from international and local civil society organizations, as well as national agencies, private companies and electoral management bodies, is also growing. It includes:

fact-checking

activities highlighting and disproving false or misleading information, which may be communicated on websites, social media or through radio stations, and are sometimes used to support other activities (such as pre-bunking, advocacy or larger public education efforts);

---

22 BBC Media Action, "Tackling Information Disorder," 2021, accessed June 6, 2024, https://downloads.bbc.co.uk/mediaaction/pdf/approaches-information-disorder-2021.pdf.

23 Access Now, "Internet Shutdowns and Elections Handbook," accessed February 22, 2023, https://www.accessnow.org/internet-shutdowns-and-elections-handbook/.

24 Nathaniel Allen and Catherine Lena Kelly, "Deluge of Digital Repression Threatens African Security," *Africa Center for Strategic Studies*, January 4, 2022, accessed March 28, 2024, https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/.

25 Eleanor Marchant and Nicole Stremlau, "The Changing Landscape of Internet Shutdown in Africa: A Spectrum of Shutdowns: Reframing Internet Shutdowns From Africa," *International Journal of Communication* 14, (2020), accessed January 23, 2024, https://ijoc.org/index.php/ijoc/article/view/15070; Phineas Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists," Forbidden Stories, July 18, 2021, accessed February 21, 2024, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

media capacity-building

interventions designed to help develop and strengthen the skills, processes and resources of media organizations so they can increase their integrity, reach and sustainability;

digital or media literacy training

efforts to build individuals' ability to think critically about the information they engage with (online or offline), by training citizens, civil society, journalists, politicians, EMBs, and other key stakeholders;

cybersecurity capacity-building

training and support that helps organizations and individuals develop mechanisms and skills to make their personnel, processes and systems more resilient to online attacks;

pre-bunking[26]

interventions (e.g., online games or broader public information campaigns) aimed at preemptively making people aware of manipulation techniques or narratives commonly found in mis- or disinformation – a "preventative" approach designed to avoid pitfalls often encountered by post-factum debunking/fact-checking;[27]

advocacy

communication strategies, bilateral meetings, coalition-building, and other efforts aimed at bringing policy change from key stakeholders, including: social media platforms, who are not doing enough about online threats emanating from their websites; governments, who weaponize online space through restrictive laws, the hiring of private contractors to subvert elections, or internet shutdowns; and the companies (such as telecom operators) who enable governments to misuse their services;

strategic litigation

the practice of bringing lawsuits meant to effect societal change, for instance by challenging the legality of internet shutdowns or demanding accountability from corporations who allow digital threats to spread.[28]

---

26 T. Harjani, J. Roozenbeek, M. Biddlestone, S. van der Linden, A. Stuart, M. Iwahara, B. Piri, R. Xu, B. Goldberg and M. Graham, "A Practical Guide to Prebunking Misinformation," (2022), accessed January 23, 2024, https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation.pdf.

27 S. Lewandowsky, U.K.H. Ecker, C. M. Seifert, N. Schwarz and J. Cook, "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 3 (2012): pp. 106—131, https://doi.org/10.1177/1529100612451018.

28 Dunia Mekonnen Tegegn, "Advancing Strategic Litigation on Internet Shutdowns Cases in Africa: Promises and Pitfalls," CIPESA, accessed June 6, 2024, https://cipesa.org/wp-content/files/Advancing-Strategic-Litigation-on-Internet-Shutdowns-cases-in-Africa-Promises-and-Pitfalls.pdf.

Methodology

This report is based on a secondary literature review, interviews conducted in-person and online, a scenario exercise using foresight methods, and three research workshops. The team sought to engage with the broadest possible range of practitioners, policymakers, academics, and other experts. The stakeholders engaged numbered over 100 and included donors and implementing organizations based across Africa, Europe and the US. The project team conducted online interviews with experts working on and in South Africa, Nigeria, Ghana, Zimbabwe, and Liberia; and traveled to Kenya, Mauritius, Tanzania, Ethiopia, and Uganda to conduct in-person interviews and attend conferences on digital issues (which brought together a large range of African CSOs, governments, academics, and donors).[29] In total, the research team conducted 73 interviews. These were complemented by two interactive workshops in Berlin, which took place in May and September 2023 (bringing together 33 participants); as well as a third workshop in April 2024, in which the team used strategic foresight methods[30] to assess plausible digital threats and explore possible programming approaches for the upcoming general elections in Mozambique (October 2024) and Ghana (December 2024) (for more information, see Appendix 2). To explore programming challenges in both contexts, the team used an expert survey (focusing on influential factors shaping the elections) to systematically develop several scenarios, which formed the basis for the one-and-a-half-day workshop with donors and implementing organizations engaged in both countries.

We chose to avoid a prescriptive vision of "success" to account for the varied nature of the threat landscape across elections and countries, and because there remains limited research into what success looks like in mitigating digital threats to elections. Instead, our selection of good cases was guided by the goal of identifying positive patterns; we asked the question, where implementers or donors deemed an intervention to have been more successful than previous efforts, what factors were present? These are the "building blocks for success" that follow.

The team focused on Africa (and particularly East Africa) to allow for both (1) understanding cross-continental efforts and (2) deeper investigation into a few national contexts (such as Kenya and Uganda). Despite the broad scope of interviews and methods that form the basis of this report, a few limitations should be noted. As a research team based in Berlin, Germany, interviewing individuals mostly based on the African continent (for a project funded by the German Federal Foreign Office), it cannot be ruled out that implicit power hierarchies biased conversations. Similarly, all interviews were held in English, thus potentially limiting the linguistic and cultural nuances that could be grasped in interviews with non-native speakers. Although we aimed to mitigate power imbalances and implicit biases by offering transparency on the project's end products and trying to build trust with our conversation partners, our positionality as researchers based in the Global North might have affected interviewees' ability and comfort to frankly share criticism or concerns derived from their work with donors, both in our online and in-person conversations.

29 The team attended the Africa Fact Check Summit (a convening of 200 fact-checking organizations in Mauritius), the Forum on Internet Freedom (largest gathering of organizations working on internet freedom in Africa, held in Tanzania), and the Kampala Geopolitics Conference (conference focus on African perspectives on geopolitical trends in the region).

30 Sarah Bressan, Håvard Mokleiv Nygård and Dominic Seefeldt. "Forecasting and foresight: Methods for anticipating governance breakdown and violent conflict," EU-LISTCO, (2019), accessed April 18, 2024, https://eu-listco.net/forecasting-and-foresight-methods-for-anticipating-governance-breakdown-and-violent-conflict/.

Mitigating Digital Risks to Elections: Building Blocks for Success

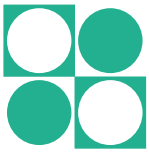
Speaking with those tackling digital election threats in Africa has yielded important lessons, which also apply to donors and implementers attempting to navigate similar threats around the world. The rest of the report will draw on these lessons by outlining four building blocks for success. Each building block will be broken down into three potential levels of investment – high, medium and low – in terms of both funding and time. This is an acknowledgment that the pot of money for such activities is finite, rather than a comment on the quality of the examples (all of which saw organizations make impressive progress under difficult conditions).

Understanding the Digital Threat Landscape

With high investment:
Baseline surveys, iterative learning & endline assessments

With medium investment:
Learning as we go (and planning for it)

With minimal investment:
Asking whether programming worked



Varied Actors for Varied Digital Threats

With high investment:
Investing in coalitions

With medium investment:
Supporting strategic coordination

With minimal investment:
Facilitating networking

Taking an Institutional Approach to Digital Threats

With high investment:
Co-design localized election work

With medium investment:
Work on gaps in institutions

With minimal investment:
Fund core capacity, not just another program

Hybrid Solutions for Hybrid Problems

With high investment:
Tailoring to the tech need

With medium investment:
Assess the capacity to use tech

With minimal investment:
Consider lower tech solutions

To examine what organizations have been able to do (as well as what they could potentially achieve) with differing levels of investment, this report will delve into each of these building blocks in turn, exploring the main challenges and some ways in which CSOs, states and international organizations have sought (or at least have started to try) to address them. In our research, we have seen the intricacies of how digital threats present themselves in different country contexts throughout the African continent. It is important to note that this report does not offer plug-and-play approaches for tackling digital threats to elections irrespective of context. Instead, it is more process-oriented: it uses examples of what has worked before to examine how policymakers can approach the unique constellation of digital and non-digital threats in the countries they are working in or on (highlighting things that must be considered and accounted for rather than things that must be done).

Building Block One: Understanding the Digital Threat Landscape

Digital threats do not impact all elections (or even all citizens) equally or in the same way: the types of threats that are most dangerous will vary across elections, political systems and societies. In democratic countries, like Kenya, mis- and disinformation are often the main challenges to electoral integrity. In other cases where parts of the election process have been digitized, such as in Nigeria, the cybersecurity of EMBs and broader electoral processes will also be a key concern. In less democratic countries, like Uganda and Ethiopia, the history of internet disruptions forces CSOs, journalists, activists, and opposition parties to plan for this eventuality.[31] In such contexts, these same actors increasingly also need to navigate online censorship and surveillance technologies.[32] For instance, according to Reporters Without Borders, two Togolese journalists were targeted by Pegasus spyware in 2021.[33] Others will have to negotiate laws and other government actions that purport to combat disinformation, but which often limit the ability of journalists, CSOs and citizens to act.[34] Focusing too much on one threat or part of one threat (for instance, online disinformation) can distort understandings of the true digital threat landscape in a country and can, in turn, undermine the ability to respond effectively.

Factors such as age, class, location, education, gender, and disability also play an important role in determining the impact of digital threats. These factors often prove decisive in whether people can even get online, and often determine levels of vulnerability once online. Elderly people and those with less experience online tend to be more susceptible to disinformation campaigns. These factors also shape potential harms to those running for office: women political candidates are disproportionately targeted by online harassment, disinformation campaigns and attacks.[35] During the 2022 Kenyan election, Martha Karua was the only prominent woman in the presidential debates – and faced targeted disinformation campaigns aimed at discrediting her candidacy.[36] In Somalia, there have been cases of women candidates

31 Fennet Habte and Abi Watson, "Europe Needs a Nuanced Approach," https://ip-quarterly.com/en/europe-needs-nuanced-approach-disinformation-african-elections.

32 Anita R. Gohdes, *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*, New York, NY: Oxford University Press, 2023.

33 Agence France-Presse, "Two Togolese Journalists Were Targeted by Pegasus Spyware, Media Advocates Say," Voice of America (VOA) Africa, January 23, 2024, accessed June 6, 2024, https://www.voaafrica.com/a/two-togolese-journalists-were-targeted-by-pegasus-spyware-media-advocates-say-/7451407.html.

34 For more information see Lexota, a database exploring how "laws and government actions against disinformation impact freedom of expression across Sub-Saharan Africa": LEXOTA (Interactive Tool), available at www.lexota.org, accessed June 6, 2024.

35 Lynn Morris (BBC Media Action), interview, Kenya, October 9, 2023.

36 Fumbua, "Fake News' in Kenya's 2022 Elections: What Has Gender Got to Do with It?," August 3, 2022, accessed June 6, 2024, https://fumbua.ke/2022/08/03/fake-news-in-kenyas-2022-elections-what-has-gender-got-to-do-with-it/.

Factors such as age, class, location, education, gender, and disability play an important role in determining the impact of digital threats.

being blackmailed and silenced by hackers who obtained photos of them with men who were not their husbands.[37] There has also been evidence of gendered attacks aimed at election workers,[38] as well as at women and gender-minority individuals who had been vocal online.[39] A report by Pollicy, a feminist civic technology organization, has shown that violence has pushed many women candidates out of the online information space, thus costing them one avenue to educate voters and engage with their constituencies.[40] These gender-based attacks tend to be part of larger strategies to discredit elections, but they too often result in shutting down women's voices and democratic participation, especially online.[41] A 2020 report on the role of gender in international cybersecurity described how even if digital violence does "not target people specifically on the basis of gender, [it] can have a more severe impact on women and LGBTIQ people because of historical and structural inequalities in power relations based on gender and sexuality."[42]

Any effort to mitigate against digital threats, then, will only work if it is clearly cognizant of and designed for the target audience. For instance, online games designed to pre-bunk dis- and misinformation are a useful way to sensitize young people (in urban areas with good internet access and a relatively high level of digital literacy) to the dangers of those digital threats, but they would be less useful for older people or those in rural areas with less access to the internet and experience using it.

To understand these dynamics, formative research is more important than ever – yet it is usually lacking and rarely given sufficient time or a distinct funding line. As one UNDP evaluation stated:

> *"Numerous interventions aimed at countering information pollution have been trialled at the local level but there are limited data, research or analysis regarding impact or possibilities for further innovation. The nature of the fast-evolving information landscape means that programmatic interventions are often hastily deployed, and follow-up is not always robust. Opportunities for learning and innovation are being lost and new trends in information pollution are often slow to be identified."*[43]

As a consequence, the authors added, "[t]oo often, failed or faulty... programs are repeated without an assessment or an evaluation of impact."[44]

---

37 Morris (BBC Media Action), interview, October 9, 2023.

38 Ingird Bicu and Hyowon Park, "Between sexual objectification and death threats: Electoral officials all over the world face unprecedented levels of disinformation, aggression and harassment," *International IDEA*, November 24, 2022, accessed February 15, 2024, https://www.idea.int/news/between-sexual-objectification-and-death-threats-electoral-officials-all-over-world.

39 Women of Uganda Network (WOUGNET) and Association for Progressive Communications (APC), "Examining the Effect of Shrinking Civic Space on Feminist Organizing Online, Particularly for Structurally Silenced Women in Uganda," December 2021, accessed February 27, 2024, https://wougnet.org/download/examining-the-effect-of-shrinking-civic-space-on-feminist-organizing-online-particularly-for-structurally-silenced-women-in-uganda/.

40 A. Kakande, B. Nyamwire, B. Saturday and I. Mwendwa, "Byte Bullies: Understanding Violence against Women in Politics and Leadership - A study on the 2022 Kenya General Elections," *Pollicy*, 2023, accessed February 15, 2024, https://vawpke.pollicy.org/.

41 UNDP Tech for Democracy (TfD), "Promoting Information Integrity in Elections: Global Reflections from Electoral Stakeholders," 2023, https://www.undp.org/sites/g/files/zskgke326/files/2023-03/Promoting%20Information%20Integrity%20in%20Elections_Global%20Reflections%20from%20electoral%20stakeholders_final_0.pdf.

42 Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security," *Women's International League for Peace and Freedom and the Association for Progressive Communications,* April 2020, accessed June 6, 2024, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

43 UNDP TfD, "Promoting Information Integrity," p. 20.

44 Ibid., p. 17.

Additionally, many interventions do not begin in time to properly understand their context, and are thus unable to develop an approach tailored to actual needs. Interviewees explained that elections are "processes not events,"[45] and should be considered as part of efforts to address broader governance issues; yet international donors tend to overly focus on the day of voting itself. Much of the funding surrounding elections is limited to a time frame of six months before and after polling day. UNDP's own assessment of its iVerify project, a fact-checking tool that can be used to identify false information and prevent and mitigate its spread, found "the impact of the tool was hampered by the short implementation timeframe that resulted in lack of awareness and, therefore, buy-in by key stakeholders, specifically journalists and civil society organisations."[46] In contrast, private contractors commissioned by electoral candidates to spread disinformation, undermine electoral integrity or foster electoral violence often begin their work shortly after the last election. One interviewee in Uganda emphasized that for many malicious actors, campaigning starts "immediately after election day."[47]

Interviewees explained that elections are "processes not events," and should be considered as part of efforts to address broader governance issues.

The huge variation in the impact of digital threats across countries and individuals, combined with the fact that efforts to learn from past mistakes (and achievements) are often poorly resourced, can mean that many interventions continue to be ineffective or counterproductive. But there have been some efforts to address this, which provide useful insights. Given these budget limits, this report looks at what can be achieved with high investment (baseline surveys, iterative learning and endline assessments), medium investment (focused on learning as ones works), and finally minimal investment (attempting to pull lessons from past efforts after the election is over).

High Investment: Baseline Surveys, Iterative Learning & Endline Assessments

The approach that the evidence suggests is most impactful, responsible and cost-effective is to: (1) run a baseline assessment of key risks and vulnerabilities before an intervention has started to develop its strategy; (2) continually learn throughout; and then (3) undertake an assessment of what was achieved at the end. To the first step, as one interviewee noted, implementers who want to craft carefully thought-out responses need to first consider what groups they are looking at, what the most prevalent narratives and harms are, and where these stem from.[48] AIfluence, a for-profit based in Nairobi that uses social media "micro influencers" to magnify messages for their clients and track responses,[49] conducts baseline surveys to identify the most important nodes of information dissemination in specific communities on certain issues, and develop strategies based on this knowledge.[50] BBC Media Action uses formative research (involving a range of methods, including large-scale surveys and qualitative research) to better understand the media ecosystem and information landscape of a particular context, including any threats from disinformation actors, prevalent mis- and disinformation narratives, and vulnerability factors for certain groups in society. It also uses research to understand how to best reach and engage a range of potential audience groups, for example by looking at what sources people trust, what types of formats they like to

45 DW Akademie Uganda representative, interview, Uganda, October 17, 2023; Irene Mwendwa and Rachel Magege (Pollicy), online interview, August 29, 2023.

46 UNDP TfD, "Promoting Information Integrity."

47 Civil society representative, interview, Uganda, October 19, 2023.

48 Alasdair Stuart (BBC Media Action), online interview, August 4, 2023.

49 "AI-Fluence," accessed June 6, 2024, https://www.ai-fluence.com/.

50 AIfluence representative, interview, Kenya, October 11, 2023.

engage with, and what attitudes and behaviors influence their engagement with information. Their research approach includes pre-testing pilot content for resonance and effectiveness, with feedback being used to make improvements before full rollout.[51] Baseline surveys thus help ensure efforts are based on evidence and cognizant of their context.

Even absent the ability to do independent research, there are many resources, guides and databases that can make this work much easier (see Appendix 1 for recommendations). For instance, the LEXOTA tracker provides analysis of laws and government actions on disinformation across sub-Saharan Africa.[52] Freedom House's annual publication, *Freedom on the Net*, surveys internet freedom around the world.[53] The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) and the African Digital Rights Network publish thorough country reports on the digital rights landscape and the state of internet freedom in individual countries.[54] Relatedly, the Centre for Democracy and Development (CDD) in Nigeria assessed the information ecosystems of West African countries, and their reports demonstrate the usefulness of understanding how information spreads.[55]

Foresight methods can help implementers explore a variety of possible developments, become aware of weaknesses and pinpoint potential future pitfalls.

Foresight methods, including scenario planning and tabletop exercises, are other ways to position an intervention for success. In several of our interviews – including with the UK's FCDO – interviewees explained that these types of exercises were being done to better prepare them and others for upcoming elections.[56] Foresight methods can help implementers explore a variety of possible developments, become aware of weaknesses and pinpoint potential future pitfalls. Participants in our strategic foresight workshop also mentioned that by using scenarios to inform program planning, they could more clearly grasp the assumptions underlying the plausible future election trajectories they were preparing for. It allowed for "safely" testing alternative future pathways, including those where programming goals would fail, without real-life consequences.[57] Basic iterations of scenario exercises can be comparatively easy to run (see Appendix 2 for more details on our methodology), but time for scenario work or similar efforts needs to be scheduled early in the process of preparing election programming and explicitly included in the planning stage.

While preparatory analysis is useful, it is rarely enough. Dynamics on the ground can change dramatically in normal times, never mind during election periods – when tensions are high, false news stories proliferate, and some governments demonstrate a greater propensity to weaponize surveillance, hacking and shutdowns to control narratives. For this reason, there is a need to build on these baseline studies to constantly learn and re-adjust.[58] Many organizations we spoke to developed systems to constantly measure and adapt to changing dynamics. Shujaaz, a Nairobi-based multimedia youth platform connecting "young people

51 Morris (BBC Media Action), interview, October 9, 2023.

52 LEXOTA (Interactive Tool), available at www.lexota.org, accessed June 6, 2024.

53 Freedom House, "Freedom on the Net," accessed June 6, 2024, https://freedomhouse.org/report/freedom-net.

54 CIPESA, "Publications," accessed April 17, 2024, https://cipesa.org/resources/?dl_page=3; African Digital Rights Network, "Publications," accessed April 17, 2024, https://www.africandigitalrightsnetwork.org/publications.

55 Idayat Hassan, "Nigeria's Fake News Ecosystem: An Overview," *Africa Portal*, February 17, 2022, accessed June 6, 2024, https://www.africaportal.org/publications/nigerias-fake-news-ecosystem-overview/.

56 FCDO representative, interview, October 6, 2023; for more information on the UK's approach to futures thinking, see U.K. Gov, "The Futures Toolkit: Tools for Futures Thinking and Foresight Across UK Government," *Government Office for Science* (2017), https://assets.publishing.service.gov.uk/media/5a821fdee5274a2e8ab579ef/futures-toolkit-edition-1.pdf.

57 Gelila Enbaye, Jakob Hensing and Philipp Rotmann, "Gaming the Political Economy of Conflict: A Practical Guide," GPPi, April 22, 2024, accessed May 2, 2024, https://gppi.net/2024/04/22/gaming-the-political-economy-of-conflict.

58 Philipp Rotmann and Abi Watson, "Close the Gap: How to Leverage Local Analysis for Stabilization and Peacebuilding,"GP-Pi, October 17, 2023, accessed June 6, 2024, https://gppi.net/2023/10/17/how-to-leverage-local-analysis-for-stabilization-and-peacebuilding.

with... information, skills and resources," has conducted over 13,000 surveys with young people since 2016. It has reported on changes in perceptions on "sexual reproductive health," "financial fitness (how to start and run a small business)," and "governance (how young Kenyans can engage with governance structures as a citizen)."[59] Access Now, a non-profit organization founded in 2009 that focuses on digital civil rights, built a database of previous internet shutdowns, offering insights into the "playbook" so that organizations can better anticipate authoritarian regimes' actions in upcoming elections.[60] Access Now also keeps and continuously updates an election and internet shutdown watchlist, aimed at tracking risks of shutdowns and monitoring areas where a shutdown has taken place.[61] For its "Uplifting Community Voices" project, DW Akademie Uganda built a system for local journalists from partnering media houses to track stories and grievances regarding public service delivery at the local community level, enabling continuous accountability reporting throughout the electoral cycle and bridging the technological communication gap between people in remote communities and the media houses that serve them.[62] By creating the necessary preconditions to iteratively learn and adapt interventions, organizations can be better equipped to keep their efforts relevant in a constantly changing environment.

Dynamics on the ground can change dramatically in normal times, never mind during election periods.

The baseline assessments and mid-programming assessments provide the evidence base for implementers to revisit an intervention after the fact to evaluate its impact. BBC Media Action uses a range of evaluation approaches for this purpose. For example, content analysis of partner media organization's content before and after capacity-strengthening support is used to assess whether supported content has improved in terms of accuracy, balance, quality, inclusion of marginalized voices, or other relevant indices of success. Measuring the impact of media content on audiences is complex, but BBC Media Action does this by tracking people's awareness and knowledge about a certain issue or topic, as well as levels of discussion, attitudes, social norms, and ultimately people's behaviors.[63] By planning evaluations and committing to follow through on them, organizations made sure to seize valuable opportunities for learning.

●● Medium Investment: Learning As We Go (And Planning for It)

Organizations are often not given enough time to conduct sufficient baseline surveys before they start an intervention and so are forced to iteratively learn, developing responses while they are working and "learning on the job." Most organizations and individuals learn on the job every day; however, it takes time (and often additional resources) to digest evidence and adapt efforts in response to what is being learned (and for these lessons to be made available to others working in the same space).[64] When small organizations already work under funding pressures, they are themselves often unable to cover the costs or find staff capacity for effective learning – instead, funding and time must be earmarked to enable this learning to happen.

59 Shujaaz Inc., "Young & Kenyan: 7 Years, 13,000 Interviews with Kenya's most important generation: An essential guide to the trends that will shape their future," February 2023, accessed June 6, 2024, https://kenyanyouthtrends.shujaazinc.com/.

60 Access Now, "Ending Internet Shutdowns," accessed April 18, 2024, https://www.accessnow.org/issue/internet-shutdowns/.

61 Access Now, "2024 Elections and Internet Shutdown Watch," accessed June 6, 2024, https://www.accessnow.org/campaign/2024-elections-and-internet-shutdowns-watch/.

62 Elisabeth Zach, "Challenges – and solutions – for rural journalism in Uganda," *DW Akademie*, May 5, 2022, accessed April 18, 2024, https://akademie.dw.com/en/challenges-and-solutions-for-rural-journalism-in-uganda/a-61682353.

63 Morris (BBC Media Action), interview, Kenya, October 9, 2023; BBC Media Action, "Our insight and impact," accessed June 6, 2024, https://www.bbc.co.uk/mediaaction/insight-and-impact/.

64 Rotmann and Watson, "Close the Gap: How to Leverage Local Analysis for Stabilization and Peacebuilding."

A useful example is the MAPEMA (Maintaining Peace Through Early Warning, Monitoring and Analysis) consortium, built with the aim of countering hate speech in the 2022 Kenyan election.[65] This has been a critical issue in Kenya, especially since the 2007 election, when ethnically biased hate speech combined with systematic vote-rigging sparked public outrage and electoral violence, leaving over 1,200 people dead and close to 300,000 displaced.[66] In every year since, there have been a number of efforts aimed at mitigating the harmful effects of hate speech and preventing such extensive national violence from repeating.[67]

By 2022, almost half of Kenyans regularly got their news online. Despite legislation and civil society efforts to curb misinformation, fake polls, fake news and deepfakes were widely circulating on social media.[68] One initiative working to counter the spread of false information was the MAPEMA consortium, which was spearheaded by Code for Africa (the continent's largest network of civic technology and data journalism labs) and coordinated by UNDP.[69] Its members included AIfluence and Shujazz, but also the National Cohesion and Integration Commission (or NCIC, a statutory body to promote national identity and values; mitigate ethno-political competition and ethnically motivated violence; eliminate discrimination on ethnic, racial and religious bases; and promote national reconciliation and healing).[70] The consortium was unable to complete a baseline survey before beginning programming around the elections and so, instead, it was provided with additional resources that made it possible to focus on learning while developing measures.

The MAPEMA consortium identified harmful disinformation and hate speech in Kenya, using a combination of in-country investigative researchers and data-driven forensic analysis, which served as an early-warning mechanism for immediate intervention by stakeholders, who shaped peace messaging and public engagement strategies.[71] Members used an array of tools to monitor online conversations, track digital media, analyze trends on social media, and identify networks involved in electoral disinformation campaigns on Facebook, Instagram and Twitter. They generated real-time reports that were used to inform "a series of counter-messaging campaigns to disseminate… messaging through traditional and online media."[72] They also developed a lexicon in English, Swahili, Sheng, and 15 other local languages – including definitions, taxonomies and benchmarking – to monitor developments related to hate speech and incitement to violence. Moreover, an actor watchlist mapped influential officeholders, identifying an estimated 17,000 candidates, 38.79 percent of whom were present on social media. To track the likelihood of violence, ILab at Code for

65 Bilal Tairou, "How Kenya's MAPEMA Project Shatters Election Deception, Builds Peace," *African Fact Check Alliance Medium*, October 30, 2023, accessed June 19, 2024, https://factcheck.africa/how-kenyas-mapema-project-shatters-election-deception-builds-peace-fafeb373e6ff.

66 Afro Barometer, "BP48: Ethnicity and violence in the 2007 elections in Kenya," February 1, 2008, accessed June 6, 2024, https://www.afrobarometer.org/publication/bp48-ethnicity-and-violence-2007-elections-kenya/; Jennifer Cooke, "Background on the Post-Election Crisis in Kenya," *Center for Strategic & International Studies*, August 6, 2009, accessed June 6, 2024, https://www.csis.org/blogs/smart-global-health/background-post-election-crisis-kenya.

67 Oren Gruenbaum, "How a handshake lost Raila Odinga the Kenyan election," *The Round Table: The Commonwealth Journal of International Affairs*, September 3, 2022, accessed June 6, 2024, https://www.commonwealthroundtable.co.uk/general/eye-on-the-commonwealth/how-a-handshake-lost-raila-odinga-the-kenyan-election/.

68 Lilian Olivia, "Disinformation was rife in Kenya's 2022 election," *LSE Blogs*, January 5, 2023, accessed June 6, 2024, https://blogs.lse.ac.uk/africaatlse/2023/01/05/disinformation-was-rife-in-kenyas-2022-election/.

69 UNDP, "Information Integrity for Electoral Institutions and Processes: Reference Manual for UNDP Practitioners," (2024), Oslo: UNDP Global Policy Centre for Governance, accessed March 29, 2024, https://www.undp.org/policy-centre/oslo/publications/information-integrity-electoral-institutions-and-processes-reference-manual-undp-practitioners.

70 National Cohesion and Integration Commission Kenya, "NCIC at a Glance," accessed February 22, 2024, https://cohesion.go.ke/index.php/about-us/ncic-at-a-glance.

71 UNDP, "Information Integrity for Electoral Institutions and Processes: Reference Manual for UNDP Practitioners."

72 Code for Africa, "Unmasking Hate Speech in Kenyan Elections with AI and Collaboration," *Code for Africa Medium*, June 12, 2023, accessed June 6, 2024, https://medium.com/code-for-africa/unmasking-hate-speech-in-kenyan-elections-with-ai-and-collaboration-576e37d4ccb5.

Africa built dashboards to help the coalition monitor spikes in the use of terms indexed in its hate lexicon.[73]

Reports were initially produced monthly, then weekly, and finally – during the week of the election – daily. AIfluence described the importance of having a "very fluid" campaign alongside social listening tools, resulting in a rapid feedback loop.[74] Members brought feedback from their network to the rest of the consortium, allowing them to stay informed of how well campaigns were working. For instance, Shujaaz's surveying of young people found a lot of confusion around how to vote; in response Shujaaz ran panel discussions, dubbed Mic Yetu (Our Microphone) events, including one where an election official sat down with young people to explain the voting process and dispel misconceptions.[75] Similarly, when Shujaaz found that campaigns focused on the main parties were losing young people's attention, the organization shifted focus to highlight the roles of local leaders like governors, women representatives and Members of the County Assembly (whose roles were felt to be more tangible).[76] This iterative learning (and adaptation) was consciously built into the Consortium when it was designed and set up, thereby enabling its members to "learn on the job."

Adapting to changing circumstances was also paramount for Ugandan organizations when the government shut down the internet ahead of the 2021 election.

Adapting to changing circumstances was also paramount for Ugandan organizations when the government shut down the internet in the leadup to the 2021 election. This election took place amid the global Covid-19 pandemic. Citing the risk of infection, the Museveni government banned campaign rallies. This increased the importance of social media's role in the election campaign.[77] After four-time presidential candidate Kizza Besigye decided not to run again, Bobi Wine, a popular singer, emerged as Museveni's main opponent. He was arrested multiple times during the campaign, resulting in violent clashes between his supporters and Ugandan security forces.[78] Shortly before the election, an investigation exposed a network of social media "puppet accounts working across Facebook and Twitter to spread disinformation about candidates challenging incumbent president Yoweri Museveni and his National Resistance Movement party."[79] When Facebook took down the accounts, the Ugandan government responded by completely shutting down internet access, causing confusion on election day. Museveni officially won the election, but many opposition parties have questioned the validity of this result.[80] To this day the government continues to block access to Facebook.

The organization WOUGNET was part of the Women's Situation Room Uganda, funded by the EU, UNDP and UN Women to train women and young people to monitor the election during this contentious time. As the country experienced a full-blown internet shutdown,

73 Civil society representative, interview, Kenya, October 12, 2023.

74 AIfluence representative, interview, Kenya, October 11, 2023.

75 DJ Boyie, "Process ya ku-vote - MicYetu," Facebook, August 1, 2022, accessed June 6, 2024, https://www.facebook.com/watch/?v=1263194811085659.

76 Shujazz representative, interview, Kenya, October 11, 2023.

77 Songa Samuel-Stone, "Digital Voter Manipulation: A situational analysis of how online spaces were used as a manipulative tool during Uganda's 2021 General Election," *Konrad Adenauer Stiftung and African Institute for Investigative Journalism*, June 26, 2023, accessed June 6, 2024, https://www.kas.de/de/web/uganda/laenderberichte/detail/-/content/digital-voter-manipulation.

78 Halima Athumani and Lesley Wroughton, "37 dead in Uganda protests after arrest of presidential candidate Bobi Wine," *Washington Post*, November 20, 2020, accessed June 6. 2024, https://www.washingtonpost.com/world/africa/uganda-protests-bobi-wine/2020/11/20/efe106ec-2aa6-11eb-9c21-3cc501d0981f_story.html.

79 Pius Enywaru and Leah Kahunde Ndung'u, "Debunking election disinformation during Uganda's internet shutdown," *Code for Africa Medium*, March 26, 2021, accessed June 6, 2024, https://medium.com/code-for-africa/debunking-election-disinformation-during-ugandas-internet-shutdown-d82f8345b634.

80 Unwanted Witness, "Unwanted Witness Publish a Briefing for Election Observers on the Importance of Privacy and Data Protection in the Election Cycle," March 29, 2021, accessed June 6, 2024, https://www.unwantedwitness.org/unwanted-witness-publish-a-briefing-for-election-observers-on-the-importance-of-privacy-and-data-protection-in-the-election-cycle/.

the previously established reporting mechanisms were no longer accessible. Instead, the program set up a toll-free number to call in the event of incidents and to maintain connections between the different monitoring regions. While many organizations have proven remarkably resourceful in the face of this kind of challenge, WOUGNET's immediate pivot to the "worst-case scenario" plan showed the importance of constantly adapting to changes on the ground.[81]

Minimal Investment: Asking Whether Programming Worked

After programming has finished, a failure to take stock of what went well (and what did not) is a wasted opportunity to learn how to improve. In addition to retrospective assessments of an election, it can be worthwhile to use the trends just seen to think through and prepare for new and emerging threats that the next election may bring. This is why UNDP undertook an evaluation of its iVerify system.[82] The review highlighted the usefulness of such assessments, providing insights into how to improve UNDP's approach.[83] Similarly, Code for Africa is working to draw lessons from its successful cooperation in the MAPEMA consortium, to see whether these same techniques can be used elsewhere. While this will only focus on Code for Africa's role and produce lessons for that organization, it is a welcome initiative that will allow others to see what transferrable lessons they could apply to different contexts on the continent.[84] Unfortunately, such assessments and evaluations continue to be the exception rather than the norm, meaning that decision-makers' ability to learn from past efforts is limited.

Building Block Two: Varied Actors for Varied Digital Threats

Despite the multi-faceted nature of digital threats to elections, there is a consistent lack of investment in coalition-building. In our research it was often acknowledged that diverse groups need to be brought together, including online and offline actors, fact-checkers, local media workers and journalists, communicators, and local, national and international organization staff. Fact-checking is an illustrative example of why gathering complementary efforts is so important: on their own, fact-checkers can lack reach; but combined with the right partners, fact-checking organizations can provide an essential diagnostic tool and form the basis of many responses (from proactive counter-messaging to media training, to support for EMBs fighting the lies being spread about them, to institutional support for CSOs and media houses).[85] For this reason, leaders and founders of fact-checking organizations in Africa, Latin America and Europe recently called on other fact-checkers to build coalitions "with politicians, the traditional media, social-media platforms, and other relevant institutions."[86]

As part of our strategic foresight exercise (see Appendix 2), we asked participants to develop strategies to mitigate threats to upcoming elections in Mozambique and Ghana: five out of

81 Civil society representative, interview, Uganda, October 16, 2023.

82 UNDP, "IVerify," accessed June 6, 2024, https://www.undp.org/digital/iverify.

83 UNDP TfD, "Promoting Information Integrity in Elections: Global Reflections from Electoral Stakeholders."

84 Civil society representative, interview, Kenya, October 12, 2023.

85 Watson, "To Save Elections From Disinformation, Fact-Checking Is Only the First Response."

86 Peter Cunliffe-Jones, Laura Zommer, Noko Makgato and Will Moy, "How Fact-Checking Can Win the Fight Against Misinformation," *Project Syndicate*, October 17, 2019, accessed June 6, 2024, https://www.project-syndicate.org/commentary/fact-checking-in-post-truth-world-by-peter-cunliffe-jones-et-al-2019-10.

six groups included coalition-building as a core part of their strategy. Each of them further acknowledged the need to plan how the different efforts within a coalition would fit together. One participant, for instance, said that "unless we have a communication plan, we will know what is going on but won't be able to do anything about it." However, perhaps quite tellingly, coalition-building was often not given a specific budget line (or received only a small amount of funding) in their mock budget allocations. When asked about these decisions, participants initially shared a sense that coalition-building could happen in the background of other efforts, and so would not cost a lot of money.

The reality is that without sufficient time commitment and funding, coalitions do not happen organically.

Unfortunately, the reality is that without sufficient time commitment and funding, coalitions do not happen organically – as the disparate efforts to tackle digital threats in many parts of Africa show. In the case of donors, there are still many coordination issues both internally between departments and externally with other countries engaging in the same space.[87] We heard that coordination meetings occasionally take place, but overworked officials tend to lack sufficiently detailed knowledge even of their own portfolio to usefully share what they are working on with others (never mind take note of their allies and partners' portfolios). Often this leaves coordination meetings as "talking shops" that people do not attend or otherwise do not fully engage with.

Relevant regional collaborations include efforts to develop guidelines on issues of cybersecurity, digital rights or data protection within the African Union. Although these had been stalled for decades, there are now signs that this might be changing. The most prominent example is the "Malabo Convention" – the African Union Convention on Cyber Security and Personal Data Protection[88] – which was first adopted in 2014 and finally entered into force in 2023. While the convention brought to light the potential for collective commitments to a less hostile digital landscape, this achievement is overshadowed by the fact that, after ten years of coordination attempts, only 15 AU member states have ratified it.[89] In a similar vein, in March 2024 the African Commission on Human and Peoples' Rights adopted the Resolution on Internet Shutdowns and Elections in Africa, signaling much-needed political will by calling on member states to "not tolerate or engage in the interruption of access to the Internet and other digital technologies targeting segments of the population or an entire population."[90] However, many of the member countries notorious for restricting internet access during past elections have not signed on, so the effects of the resolution remain to be seen.

There are also few incentives for implementing organizations to coordinate efforts when engaging in the same election, which can lead to significant duplication in programming. For instance, many local, national and international organizations run training on digital threats (such as digital safety and literacy, fact-checking or journalistic ethics). Some interviewees complained about the low quality of training,[91] yet we only found limited examples (such

87 Abi Watson and Megan Karlshøj-Pedersen, "Fusion Doctrine in Five Steps: Lessons Learned from Remote Warfare in Africa," *Saferworld*, November 2019, accessed June 6, 2024, https://www.saferworld.org.uk/resources/publications/1295-fusion-doctrine-in-five-steps-lessons-learned-from-remote-warfare-in-africa; Rotmann and Watson, "Close the Gap: How to Leverage Local Analysis for Stabilization and Peacebuilding.

88 African Union, "African Union Convention on Cyber Security and Personal Data Protection," accessed May 28, 2024, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

89 Nnenna Ifeanyi-Ajufo, "The AU took important action on cybersecurity at its 2024 summit – but more is needed," *Chatham House*, February 23, 2024, accessed 28 May, 2024, https://www.chathamhouse.org/2024/02/au-took-important-action-cyber-security-its-2024-summit-more-needed.

90 African Commission on Human and Peoples' Rights,"Resolution on Internet Shutdowns and Elections in Africa," ACHPR. Res. 580 (LXXVIII) 2024, March 20, 2024, accessed May 28, 2024, https://achpr.au.int/en/adopted-resolutions/580-internet-shutdowns-elections-africa-achprres580-lxxvii.

91 DW Akademie Uganda representative, interview, Uganda, October 17, 2023; Enywaru Pius (PesaCheck), interview, Uganda, October 18, 2023; Session Forum on Internet Freedom, Tanzania, September 27—29, 2023.

as DW Akademie Uganda's pool of trainers) of efforts to build a common standard, offer guidance or at least share best practices between organizations providing similar training. In most cases, organizations struggling for funding were disincentivized from working with others, as they could receive funding to establish new training courses and write new guidance – even though many packages already existed and some of these initiatives would not be adding something usefully new.

This phenomenon is not unique to training on digital threats: there also appears to be a lot of duplication in fact-checking initiatives. Many countries in Africa now have at least one fact-checking organization, and while there have been some efforts to coordinate their work, many organizations run fact-checks independently and end up debunking the same lies or misleading statements at the same time as each other. Some argued that there are benefits to a few organizations flagging the same facts, amplifying their findings among their networks to validate the debunking effort, but there is a risk that this wastes limited resources and staff time.[92]

Advocacy efforts with states and tech platforms also remain poorly coordinated. This matters because, as has been extensively discussed elsewhere, tech platforms are not investing sufficient staff (especially with local language skills) or resources into content moderation in African countries compared to North America and Western Europe.[93] Added to this, advocating for the platforms to change is challenging everywhere (as one commentator notes, "social media platforms know they profit from the spread of disinformation, while advertisers turn a blind eye"[94]), but it is especially hard outside of Europe and the US. Odanga Madung, a Fellow at the Mozilla Foundation, states that the "policies and values of these platforms have normalized a kind of deviance – one that enables a dismissal of regions and populations that fall in its 'rest of the world' category."[95] While Facebook has been forced to comply with Germany's costly requests to remove content violating its national laws, it has largely dismissed demands originating from African leaders and legislators.[96] Coordinating advocacy for change would thus be key for addressing digital threats to elections on the continent.

Unfortunately, this much-needed "united front" of CSOs, policymakers and other key stakeholders (not just in Africa but around the world) is still lacking. Several organizations told us they were engaging with some tech platforms through bilateral meetings or roundtables. These meetings often focused on similar demands: better content moderation and closer engagement with civil society, to flag dangerous content or examine its impact on

92 Idayat Hassan and Jamie Hitchen, "If Blackouts Don't Work, What Might? Tackling Fake News in West Africa," *African Arguments*, July 19, 2022, accessed June 6, 2024, https://africanarguments.org/2022/07/if-blackouts-dont-work-what-might-tackling-fake-news-in-west-africa/.

93 Odanga Madung,"Kenya's Already Fragile Elections Now Face a Dangerous New Enemy: Big Tech Platforms," *The Guardian*, April 7, 2022, accessed June 6, 2024, https://www.theguardian.com/commentisfree/2022/apr/07/kenya-elections-2022-big-tech-platforms; Andrew Deck, "AI moderation is no match for hate speech in Ethiopian languages," *Rest of World*, June 27, 2023, accessed January 25, 2024, https://restofworld.org/2023/ai-content-moderation-hate-speech/; Chiagozie Nwonwu, Fauziyya Tukur, and Yemisi Oyedepo,"Nigeria Elections 2023: How Influencers Are Secretly Paid by Political Parties," *BBC News*, January 18, 2023, accessed June 6, 2024, https://www.bbc.com/news/world-africa-63719505; Martin K. N. Siele, "'It's Been Tough for Us': Meta's Kenyan Content Moderators Say They'll Keep Fighting," *Rest of World*, May 22, 2023, accessed June 6, 2024, https://restofworld.org/2023/meta-content-moderators-kenya-fired-unionize/; Nita Bhalla, "Meta urged to boost Africa content moderation as contractor quits," *Reuters*, January 24, 2023, accessed January 25, 2024, https://www.reuters.com/world/africa/meta-urged-boost-africa-content-moderation-contractor-quits-2023-01-24/.

94 Carlos Diaz Ruiz, "Disinformation is part and parcel of social media's business model, new research shows," *The Conversation*, November 23, 2023, accessed June 6, 2024, https://theconversation.com/disinformation-is-part-and-parcel-of-social-medias-business-model-new-research-shows-217842.

95 Madung, "Kenya's Already Fragile Elections Now Face a Dangerous New Enemy."

96 Iginio Gagliardone and Nicole Stremlau, "It's Time to Revisit the Framing of Internet Shutdowns in Africa," *Carnegie Endowment for International Peace*, November 21, 2022, accessed June 8, 2023, https://carnegieendowment.org/2022/11/21/it-s-time-to-revisit-framing-of-internet-shutdowns-in-africa-pub-88406.

already marginalized groups. However, in many cases our interlocutors could not engage all platforms, or else platforms' engagement petered off after meeting or after the election had ended. Interestingly, among the organizations we spoke with, it was clear that most of the tech platforms had been involved in meetings (including Meta, Twitter, Microsoft, Google, and Tik Tok), but that they had not all met with the same organizations – speaking to the opportunity wasted by failing to coordinate.[97] In fact, some felt that tech platforms were consciously seeking to fragment efforts by pursuing disparate conversations with different organizations; this allowed the platforms to give the impression that they were engaging with external concerns while minimizing the impact of collective advocacy for change.

There is, then, a need to better coordinate efforts by local, national and international organizations working on the same issues and conducting the same activities. Again, there have already been some relevant examples with varying levels of investment. The rest of this section details what can be achieved with high investment (where funders and organizations built shared coalitions to work together on digital threats facing elections), medium investment (where there has been strategic coordination around shared objectives), and low investment (where organizations have built spaces for networking to facilitate collaboration absent the funding and time needed to pursue more ambitious objectives).

High Investment: Investing in Coalitions

Instead of actively encouraging "one man shows" through funding models aimed at single organizations working alone, donors can facilitate coalition-building by properly resourcing and incentivizing the right efforts. Interviewees from CSOs consistently agreed that the most effective response to digital threats against elections is a "multi-pronged approach," which includes "fostering and enabling connection and coalition-building." They noted that this was an area that merits more resourcing, since the varied nature of threats means this is "what you need to do to be effective."[98] This type of funding, however, is not the same as forcing organizations to build coalitions – or dictating specifically who should be involved – which has caused problems in other areas of programming.[99] Instead, it means shifting the model away from individualistic funding structures to funding that provides space for coalition-building activities, which resource time for organizations to come together to examine their own capacity gaps, work with other organizations who can fill them, and plan programming with collective resources. According to interviewees, measures that more successfully tackled the multiple threats facing an upcoming election consisted of broad coalitions which consciously thought through the different perspectives, backgrounds and expertise they would need – and planned how each of their efforts could be complemented and built upon. Three ways we saw this take place was through efforts to bring together (1) offline and online actors, (2) fact-checkers and communicators and (3) local, national and international actors.

To the first of these, organizations with expertise in the online space (whether in digital security training, advocating for access to information or tracking the spread of online lies and hate) will have limited impact unless they partner with organizations focused on mitigating harms offline (such as community radio stations, police, community responders,

97 HerInternet representative, online interview, August 17, 2023; Civil society representative, interview, Kenya, October 12, 2023.

98 BBC Media Action Tanzania representative, interview, Tanzania, October 2, 2023.

99 Jakob Hensing, Melissa Li, Julia Friedrich and Philipp Rotmann, "Supporting Civil Society in Acute Crises," *GPPi*, March 14, 2023, accessed June 6, 2024, https://gppi.net/2023/03/14/supporting-civil-society-in-acute-crises.

election monitors, those conducting civic voter education, or independent election bodies).[100] This was a key focus of the MAPEMA consortium, where the response was developed by "a whole ecosystem" of local civil society organizations (like Code for Africa), a social venture (like Shujaaz), for-profit companies (like AIfluence), international organizations (including UNDP and Amnesty International), and national actors (including the National Cohesion and Integration Commission, who deployed 200 cohesion monitors). The nature of the coalition meant that information learned about rises in hateful language or changes in public attitudes could be quickly acted on, either by working with police officers and religious leaders or by taking claims to the NCIC. In the MAPEMA consortium, these actors were convened because they were seen to be the most appropriate and useful stakeholders. Their success reflects the strengths of convening a context-specific, carefully considered group of actors, where each member adds a necessary competency to effectively mitigate digital threats.

Locally developed solutions are most effective when connected with national actors who have the power to do something about it.

To the second type of relevant actors, fact-checking initiatives are important as they provide evidence against dangerous information, but they depend on trusted intermediaries such as journalists or influencers to amplify this evidence.[101] This was a key factor for success when UNDP partnered its iVerify system with community radio stations in Sierra Leone to ensure that locally trusted and owned organizations were the ones amplifying credible counter-information.[102] BBC Media Action trained the iVerify fact-checking team, and then linked them to its local media partners in order to improve the dissemination of fact-checked content throughout the country. This pattern was again evident in the MAPEMA consortium, where fact-checking efforts were combined with communication strategies. They reached over 27.9 million Kenyans after recruiting 3,000 micro- and nano-influencers "to speak actively against hate speech and to promote peaceful messaging," as well as disseminating positive messaging through traditional and online media.[103]

Finally, it is important to connect local, national and international efforts to attain more effective responses. Locally developed solutions are most effective when connected with national actors, so that what civil society is learning can be brought to those with the power to do something about it. One good case example from our interviews was the Women's Situation Room Uganda, which convened Ugandan civil society organizations to work collectively on monitoring and countering electoral violence in 30 districts, namely by training women and young people in election observation and peacebuilding. The project members identified districts that were likely to see renewed electoral violence in 2021, based on their experiences during the 2016 election. In these places, the trained "peace advocates" worked together with the Ugandan police both ahead of and on election day, to observe proceedings at the polling stations and report threats and cases of electoral violence. Observations were then passed on to the Women's Situation Room.[104] Intentionally including national actors in their work on electoral violence meant that observers had access to an actor who would be able to respond.

Similarly, international efforts to tackle digital threats to elections benefit from working with local actors, who can assess which policies are most likely to work, how certain communities may be uniquely impacted, and also leverage existing relationships. In the other direction, international organizations can also provide cover to local organizations who may face

100 BBC Media Action Tanzania representative, interview, Tanzania, October 2, 2023.

101 Watson, "To Save Elections From Disinformation, Fact-Checking Is Only the First Response."

102 BBC Media Action, "iVerify Project - Sierra Leone," The Communication Initiative Network, September 28, 2023, accessed June 6, 2024, https://www.comminit.com/global/content/iverify-project-sierra-leone.

103 Code for Africa, "Unmasking Hate Speech in Kenyan Elections with AI and Collaboration."

104 Civil society representative, interview, Uganda, October 16, 2023.

pushback from incumbent regimes for calling out their lies or not toeing the party line. BBC Media Action recognized this dynamic when teaming up with local radio stations, as they found not only that their programming benefitted from the stations' networks, but also that they had a role to play by publicly taking responsibility for decisions around what messages were and were not aired. In one West African country, BBC Media Action reported that local partner radio stations often found it useful to cite the "BBC editorial policies" they were now hewing to when challenged by local politicians who sought to use these stations to spread partisan messaging.

Another example comes from the Media Institute of Southern Africa (MISA), whose country chapters support election monitoring in MISA's 11 member countries. An interviewee from a MISA chapter explained that ahead of elections in one country, journalists affiliated with MISA physically travelled there to support their peers with election observation and reporting. The presence of journalists from neighboring countries is understood to have reduced the likelihood of violence against local reporters, due to concern over potential negative repercussions should foreign journalists be harmed.[105] Of course, this may not always be true, as in some cases a perception of Western-backed democracy promotion could worsen the economic situations of local CSOs or even put their staff in danger. For instance, the Democratic Governance Facility, a European basket fund that was a significant source of funding for organizations and government institutions working on good governance in Uganda, was suspended in January 2021 by the Museveni government based on claims that it was "used to finance activities and organizations designed to subvert [the] Government under the guise of improving governance."[106]

Any efforts at building (and maintaining) coalitions also benefit from having a convener to bring these organizations together as effectively as possible. In our interviews with MAPEMA consortium members, many noted the importance of a central convener that was not a project implementer but an organization focused on helping others successfully work together. The benefits of investing in the distinct role of a convener, be it a coalition member or an external partner, were also mentioned by interviewees from the African Internet Rights Alliance (AIRA). AIRA was born out of a group of (former) Ford Foundation grantees working on digital rights on the African continent. The alliance sought to be more deliberate in how it convened members and strategically worked together, so it created the role of convener to support the regularity of meetings, mutual learning and organizational development, as well as to facilitate more international engagement for its members.[107] Similarly, AFEX, the African chapter of the International Freedom of Expression Exchange (IFEX), a global network of over 100 organization working on freedom of information and expression, coordinates the efforts of African organizations who work on issues of digital literacy, access to information legislation and journalism training.[108] The network is facilitated by a designated secretariat, which is currently hosted by the Media Foundation for West Africa (MFWA) in Ghana, one of the coalition members. Irrespective of the model, designating resources to maintain and coordinate a coalition is necessary to ensure successful long-term coalition work.

It is encouraging to see many funders already recognizing the need to build more innovative coalitions to face new challenges. For instance, USAID will provide up to $2.5 million to launch a Coalition for Securing Electoral Integrity, which will bring together governmental

105 Civil society representative, online interview, November 2, 2023.

106 Freedom House, "Uganda: Suspension of Democratic Governance Facility Highlights Growing Concerns," February 4, 2021, accessed April 19, 2024, https://freedomhouse.org/article/uganda-suspension-democratic-governance-facility-highlights-growing-concerns.

107 African Internet Rights Alliance (AIRA) representative, online interview, November 8, 2023.

108 AFEX, "About Us," accessed June 6, 2024, https://www.africafex.org/about-us; AFEX, Online Interview September 15, 2023.

and non-governmental partners within the international electoral integrity community to develop norms, guiding principles and codes of conduct on crucial electoral integrity issues, and promote adherence to these same standards. However, the success of such an effort will depend on whether the coalition enlists key actors and whether it truly facilitates shared working between them.[109]

Medium Investment: Supporting Strategic Coordination

Even when it is not possible to establish coalitions, the nature of digital threats necessitates more strategic coordination between states, CSOs, international organizations, and other key stakeholders working to mitigate the risks of digital threats to elections. There have already been some promising improvements in this direction, like the Freedom Online Coalition (FOC), "a multi-stakeholder effort to support internet freedom and promote human rights online."[110] The FOC, founded in 2011, is a partnership of 39 governments working to advance internet freedom. Coalition members work closely together to coordinate their diplomatic efforts and engage with civil society and the private sector to globally advocate for free expression, association, assembly, and privacy online.[111] The FOC has, for instance, helped establish initiatives like the Digital Defenders Partnership (discussed more below). While already important avenues for negotiation and debate, these forums also provide the means to advance currently faltering conversations around how to improve programming against digital election threats. In 2022, UNDP launched the Action Coalition for Information Integrity in Elections, a global platform for exchange among electoral support stakeholders that aims "to build a collective understanding of the challenges and responses to information pollution impacting electoral processes."[112] In the absence of co-implemented programming, strategic coordination can thus help consolidate disparate efforts to tackle the same issues.

In the absence of co-implemented programming, strategic coordination can help consolidate disparate efforts to tackle the same issues.

In some countries there is also coordination between international donors. For instance, we heard that in Mozambique there are meetings where the main donors come together to discuss what they intend to fund in the upcoming election. This helps to identify the remaining funding gaps – and gives other donors the opportunity to address them (of course, whether other donors do address these gaps is another issue). Unfortunately, we also heard that this tends to be the exception rather than the rule; more often, desk officers are unlikely to have the capacity to properly coordinate their activities.

There is also already some impressive work by CSOs to build more collective advocacy in the face of rising digital threats to elections. The Global Coalition for Tech Justice, convened by Digital Action, aims to engage in collective action for accountability and protective frameworks, so that Big Tech companies play their role in protecting elections and citizens' rights around the world and "particularly in the global majority where companies... have been negligent in dealing with the impacts of their social media and messaging products."[113]

109 The White House, "Fact Sheet: Announcing the Presidential Initiative for Democratic Renewal," December 9, 2021, accessed June 6, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/09/fact-sheet-announcing-the-presidential-initiative-for-democratic-renewal/.

110 Ibid.

111 "Freedom Online Coalition," accessed June 6, 2024, https://freedomonlinecoalition.com/.

112 UNDP, "Defending Information Integrity: Actions for Election Stakeholders," March 20, 2024, accessed May 19, 2024, https://www.undp.org/policy-centre/governance/publications/defending-information-integrity-actions-election-stakeholders.

113 Digital Action, "Year of Democracy: Protecting Elections Globally From Big Tech," July 7, 2023, accessed January 25, 2024, https://digitalaction.co/projects/year-of-democracy/.

The International Fact-Checking Network has been working with its members from around the world to expand the reach of "wins" against tech companies in Europe and the US to contexts like the African continent, where US-based tech companies are less engaged. A key aspect of the conversation in the 2023 Africa Facts Summit, a convening of African fact-checkers, was how to ensure provisions from the Digital Services Act – an EU regulation regarding illegal content, transparent advertising and disinformation, aiming "to create a fairer and safer online world" – could be used to advocate for change in Africa, too.[114]

The global #KeepItOn coalition unites 243 civil society organizations from 105 countries to monitor, document and push back against internet shutdowns across the globe "using strategic advocacy and litigation."[115] In some cases, such as Ghana and Benin, they have managed to get governments to commit to keeping the internet on; in others, like Cameroon and Togo, they have sought legal interventions against existing shutdowns.[116] These efforts have recognized that, while most organizations will continue to work separately, pooling evidence and putting forward shared asks can be powerful advocacy tools when seeking accountability and change from tech platforms and authoritarian states.

Minimal Investment: Facilitating Networking

Several initiatives have facilitated networking and joint-learning opportunities to improve collaboration despite pressure on participating organizations' budgets and staff time. Conferences have been one common way to establish learning across different national contexts. One example is the Forum on Internet Freedom in Africa, which brings together various actors working on digital rights. Over the last decade, it has been convened by the Uganda-based Collaboration on International ICT Policy for East and Southern Africa (CIPESA). The forum allows those working on internet freedom and digital rights to connect with each other and creates opportunities for shared learning and advocacy.[117]

Since 2013, the Digital Rights and Inclusion Forum (DRIF) has been hosted by the Paradigm Initiative, a Nigeria-based digital rights and inclusion organization with offices in the Democratic Republic of Congo, Kenya, Nigeria, Senegal, Zambia, and Zimbabwe. The DRIF convenes governments, CSOs, technologists, and industry specialists with a particular focus on privacy, inclusion and access in the digital space.[118]

Finally, Africa Check also runs an Africa-based summit focused on facilitating bilateral relationships and running workshops where member organizations can exchange lessons and reflect on each other's experiences.[119] These and other CSO-run conferences were mentioned multiple times as useful spaces to exchange contacts and build space for shared learning in the future. Unfortunately, funding has limited the ability to systematically run such formats and so their impact can be short-lived.

---

114 European Commission, Directorate-General for Communications Networks, Content and Technology, "The Digital Services Act (DSA) explained – Measures to protect children and young people online," *Publications Office of the European Union*, 2023, accessed June 20, 2024, https://data.europa.eu/doi/10.2759/576008.

115 Access Now, "#KeepItOn: frequently asked questions," accessed February 23, https://www.accessnow.org/campaign/keepiton/keepiton-faq/.

116 Ibid.

117 CIPESA representative, interview Uganda, October 17, 2023; "FIFAFRICA," accessed January 25, 2024, https://internetfreedom.africa/about/.

118 Paradigm Initiative, "About DRIF," accessed April 18, 2024, https://drif.paradigmhq.org/about-drif/.

119 Africa Check, "PRESS RELEASE: Mauritius to host the 2023 Africa Facts summit," July 14, 2023, https://africacheck.org/fact-checks/blog/press-release-mauritius-host-2023-africa-facts-summit.

Others have used national co-working spaces for media and media-related organizations to connect with others. There are several national organizations – such as Bazara Media in Kenya and the MCI Media Hub in Kampala, Uganda[120] – who provide collaborative co-working spaces and also organize meetings, trainings and research support for shared advocacy, in order to amplify messaging and campaigns. Funders should consider how to support these coalitions as well as physical convening spaces and encourage grantees to lean on existing efforts rather than outline plans to be delivered on by them alone.

Building Block Three: Taking an Institutional Approach to Digital Threats

Too often, efforts to mitigate the impact of digital threats to elections focus on small-scale activity, which is at best ineffective and at worst harmful to the institutional capacity of CSOs. CSOs from and working in the area where international programming is being deployed are essential for building an ecosystem that can combat digital threats well before funding has come in for the next election, and well after everyone has voted. They understand the lies that are most insidious, including those in local languages that stoke ethnic grievances. They understand many of the nodes of mis- and disinformation, and the means through which they are spread. They understand how to focus efforts, whether to, for instance, prepare for an internet shutdown or focus on protecting civil society groups against surveillance and hacking. What is more, locally based or locally owned CSOs are in many cases more likely to be a trusted voice; state-led or internationally led efforts that do not engage with those impacted do not earn this trust and therefore rarely succeed.

These same CSOs consistently struggle to access international funding and when they do, it tends to be shorter-term funding earmarked for delivering projects rather than core costs.[121] The fickleness of funding was a recurring theme in interviews. When the Museveni government closed the Democratic Governance Facility in Uganda, this signaled an overall decline in media, civil society and election-related funding.[122] The multi-donor facility had been established by Austria, Denmark, Ireland, the United Kingdom, Netherlands, Norway, Sweden, and the European Union to support civil society organizations and government bodies in promoting good governance and strengthening the rule of law (with approximately $350 million spent between 2018 and 2022).[123] Civil society organizations perceived this and similar shifts in donor engagement and interest as handing a win to authoritarian governments, resulting in narrower civic space and, in some cases, difficulty in recovering from the loss of established funding sources.[124]

Even in less extreme cases, core funding is rarely extended. As one interviewee in Liberia told us, "our work cannot go too long, because you run out of funding when projects run out."[125] Many of the organizations we spoke to have enough funding for a few staff members to run

120 "Media Challenge Initiative," accessed January 25, 2024, https://www.mciug.org/.

121 Assitan Diallo and Delina Goxho, "Donor dilemmas in the Sahel: How the EU can better support civil society in Mali and Niger," *Saferworld*, March 2023, accessed June 6, 2024, https://www.saferworld-global.org/resources/publications/1421-donor-dilemmas-in-the-sahel.

122 Geofrey Serugo, "Democratic Governance Facility exits, leaving thousands jobless," *The Observer*, June 7, 2023, accessed April 19, 2024, https://observer.ug/news/headlines/78087-democratic-governance-facility-exits-leaving-thousands-jobless.

123 Nathan Vandeputte, "The Suspension of the Democratic Governance Facility in Uganda: The Illusion of 'Politically Smart Aid,'" *Development in Practice* 34, no. 3 (2023): pp. 336–50, https://doi.org/10.1080/09614524.2023.2238915.

124 Civil society representative, interview, Uganda, October 19, 2023; CIPESA representative, interview, Uganda, October 17, 2023.

125 Civil society representative, online interview, August 2, 2023.

projects, but rarely enough for aspects like cyber resilience or mental health support. The work of many CSOs in Africa exposes them to online and offline harm, especially when they challenge state elites or campaign against entrenched gender norms, making them targets for state repression, cyberattacks and smear campaigns.[126] Yet few have the institutional capacity to push back against lies or protect themselves against attacks and surveillance. Others – such as fact-checkers and organizations working to track and act against hate speech – must sort through shocking, graphic and traumatic content to attempt to prevent it from reaching the wider public. This all takes a toll on staff members' wellbeing, but CSOs consistently lack the sort of funding they would need to offer mental health support.[127]

Meanwhile, individualized trainings for some CSO staff, journalists and members of political parties have become a "go-to" in the international community's toolbox. But given the importance of investing in the wider institutional ecosystem, such training is not just a less good option; it is actively counterproductive.[128] While they may offer some individuals useful skills, they tend to bring these skills back to institutions that lack the capacity to facilitate them further, and any potential for improvement is lost. For instance, in previous initiatives by the Digital Defenders Partnership (DDP), they provided individual training on digital safety and harm-reduction measures and asked participants to multiply their learnings within their organizations. DDP moved away from this approach after these newly skilled staff began taking new jobs with higher salaries, leaving their former organization without their accumulated institutional knowledge; and in those cases where participants did stay, they often did not have the institutional buy-in needed to push for internal change.[129] DDP is the rare case of an implementer learning from its approach and developing impactful programming (discussed more below); too many international donors carry on funding individualized trainings despite dubious outcomes and the fact that institutions could use the same funding to address some gaps more sustainably.

Given the importance of investing in the wider institutional ecosystem, individual training is not just a less good option; it is actively counterproductive.

Instead of focusing on small-scale interventions (which train a few individuals), more should be done to help CSOs to improve their institutional capacity and sustainability, so that they can work on digital threats to democracy and governance (even when international funding largely declines after election day). Again, this need not only happen within large budgets; in our own interviews we saw work being conducted at varying levels of investment. With high investment, as we have seen start to happen with USAID, donors should look to co-design projects with local CSOs to put them in the lead in deciding how to invest money. With medium investment, training should focus not on individual capacity but rather on accompanying CSOs as they address their institutional gaps over a 6-to-12-month timeframe. With minimal investment, donors should try to address their partners' organizational gaps with their allotted funding, rather than just fund another project.

126 Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists."

127 Enywaru Pius (PesaCheck), interview, Uganda, October 18, 2023; Civil society representative, online interview, November 2, 2023.

128 International Crisis Group, "Chad's Transition: Easing Tensions Online," December 13, 2022, accessed June 6, 2024, https://www.crisisgroup.org/africa/central-africa/chad/b183-chads-transition-easing-tensions-online; Monika Benkler, Annika S. Hansen and Lilian Reichert, "Protecting the truth: Peace operations and disinformation," *Center for International Peace Operations (ZIF)*, October 2022, accessed June 6, 2024, https://reliefweb.int/report/world/protecting-truth-peace-operations-and-disinformation; MINUSCA,"Media and Civil Society Leaders Briefed on Tackling Disinformation," June 22, 2021, accessed June 6, 2024,https://minusca.unmissions.org/en/media-and-civil-society-leaders-briefed-tackling-disinformation.

129 Digital Defenders Partnership (DDP) representative, online interview, July 25, 2023.

High Investment: Co-Design Localized Election Work

It is increasingly clear that local CSOs need to have a say in the design and implementation of programs. Ideally, project partners that are trusted in the community need to be identified early on and engaged in the initial development phases. This helps ensure that activities are relevant to the context and that civil society actors are engaged as decision-makers, not just as implementers of pre-designed measures. USAID has recognized this lesson, and has committed to ensuring that by 2030 "fifty percent of our programming will place local communities in the lead to set priorities, codesign projects, drive implementation, or evaluate the impact of our programs."[130]

USAID put its localization agenda into practice in the 2022 Kenyan election, where it exclusively worked with local organizations. The focus of the project was to "support civil society and youth to successfully participate in democratic processes; lead voter and civic education and implement local strategies to mitigate and prevent electoral violence." Despite some issues in organizational capacity (discussed below), interviewees involved in this process described the experience of working with local partners very positively. For instance, the rollout of funding started later than expected, but the fact that CSOs were based within communities meant that they could quickly build on established networks, identify key issue areas and start programming much faster and more effectively than international organizations. Of course, this is still far short of co-designing programs but, combined with USAID's benchmarks for 2030, it is at least a step in the right direction.[131]

Medium Investment: Work on Gaps in Institutions

Institutional training should be prioritized over the training of a few individuals. Learning from past approaches, DDP developed the digital security accompaniment program, which – among other features – involves a DDP staff member embedding into an organization for three to six months, performing needs- and skills-assessments for each staff member and supporting the process of implementing institutional digital security measures. This long-term accompaniment program sometimes lasts nine months, and aims to raise capacity in the entire organization rather than only in selected individuals. For its accompaniment programs, DDP prioritizes organizations working on feminist, LGBTQ, environmental, and youth issues, as well as actors that make data available to the public (through radio, podcasts, blogs, or published datasets), recognizing that these groups are likely to face heightened scrutiny and possibly repression for their work challenging the status quo.[132]

BBC Media Action also takes an institutional approach: its journalist training programs in Kenya, Somalia, Sierra Leone, and elsewhere seek to address the key issues facing their local media partners, instead of merely sending a few individuals on a training course. BBC Media Action Journalism Mentors work with local media partners over a prolonged period, focusing on providing holistic support to address their partners' range of issues. BBC Media Action Tanzania, for example, offers capacity training, commercial training on how to financially operate the station, support on setting editorial standards, and production skills training. This way, partners can improve their reach and engagement with local audiences,

130 USAID, "Localization," accessed June 6, 2024, https://www.usaid.gov/localization.

131 Ibid.

132 Digital Defenders Partnership (DDP) representative, online interview, July 25, 2023.

meet their needs, and improve the quality and impact of their programming. For example, some mentors will work with each partner station for one week per month over the course of a full year. In other instances, they may work full-time with a partner station's entire team for a period of six or more months.

Minimal Investment: Fund Core Capacity, Not Just Another Program

Interviewees also mentioned examples of international donors focusing on smaller gaps in organizational capacity when running programs, recognizing that addressing these is often more impactful for local CSOs than funding another project that will fizzle out in six months. These types of investments varied quite significantly but all stemmed from the recognition that organizational capacity is a pressing issue for local CSOs and that, as international funders, there is much more they could do to address it. In that sense, these investments offer an insight into how donors can think more innovatively about the gaps local CSOs face.

One approach taken by some donors is to share the burden of core functions during the life of projects. USAID delivered on its commitment to fund only local CSOs for the 2022 Kenyan election by covering the capacity gap of local partners. Small organizations tended to lack monitoring, evaluation and learning capacity, so USAID worked with partners to provide some of this capacity (through USAID staff) so that partners could focus on delivering their projects.

Other donors have dedicated funding streams just for covering core capacity. Packard Foundation, recognizing "that historically under resourced organizations have also received the least support for capacity and leadership," focuses on leadership training, organizational strengthening, building networks with others working on similar issues, and creating resource hubs "based in geography that provide bite-sized, adaptive, and responsive training, coaching, and peer support on an ongoing basis to all grantees within that geography."[133]

Supporting core-capacity-building in organizations, especially in those established more recently, together with strengthening measures aimed at institutional sustainability, can help support an ecosystem of resilient, diversly resourced and well-capacitated organizations. These features are ever more important in the face of crackdowns surrounding elections, when inspiring efforts to support CSOs' core functions are still falling short. For instance, mental health support for fact-checkers was an issue constantly raised in interviews and could be a core capacity to focus on. Unfortunately, we did not hear any examples of this kind of work.

Building Block Four: Hybrid Fixes for Hybrid Problems

Digital threats to elections are inherently tied up with offline threats. For instance, online attacks are just one kind of violence that journalists, human rights defenders, opposition politicians, and other public figures may face. While human rights defenders encounter online harassment and doxing (publishing private or identifying information about a particular individual on the internet), they tend to also have reasons to fear offline threats to their physical safety (including break-ins at their office or their coworkers being physically intimidated, harassed or even arrested). Similarly, central issues that impact

133 The David and Lucile Packard Foundation, "Civil Society and Leadership Initiative," accessed February 29, 2024, https://www.packard.org/what-we-fund/civil-society-and-leadership-initiative/.

people's perception of electoral integrity and their ability to safely participate in elections – like discrimination, a lack of identification documents or the inaccessibility of polling stations – are situated in the offline space. This means that an online-only approach to safeguarding elections will rarely be able to live up to its aim. Added to this, online work becomes impossible when authoritarian regimes shut down the internet, as many of our interviewees experienced during election times. This informs their preparation for future elections, where a renewed surge of internet restrictions is probable.

Central issues that impact people's perception of electoral integrity and their ability to safely participate in elections are situated offline.

And yet, despite these considerations, there are many commentators, practitioners and experts proposing online-only or high-tech solutions to election threats. This was noted by Full Fact in reference to AI: "there are a lot of people who say that artificial intelligence and machine learning is a panacea, but we have been at the front lines of fact checking since 2010, we know how difficult fact checking is firsthand."[134] This echoed our own conversations with Africa-based CSOs, some of whom complained that a major funder was exclusively asking for "AI-based approaches to fact-checking," even though these same CSOs – having learned from past efforts – had started to develop more effective, lower-tech solutions to mis- and disinformation.[135] Unfortunately, it seemed likely they would be forced to develop less effective "AI-focused solutions" to access funding. Relatedly, some interviewees were skeptical of technical tools developed by international organizations now being used across Africa, as they felt they were often not based on need but on a desire to create a technical fix.

Efforts aiming to digitize election-related processes (such as civil and voting registries, or the verification, counting and transmission of votes) are a case in point. Digitized processes are increasingly being rolled out across the African continent.[136] These technologies and software are often pushed forward with the promise of more transparency, less manipulation and cost savings – thus seemingly boosting the integrity of (and public trust in) an election by way of technology. As Nic Cheeseman, Gabrielle Lynch and Justin Wills explain: "where elections are problematic – because of malpractice, or procedural problems, or both – digital technology is seen as a fix, able to compensate for the weakness of the state and to deter malpractice by politicians and officials."[137]

However, in many cases systems have been rolled out without assessing "the financial and organizational implications in terms of future updates, equipment replacement and the EMB's capacity to maintain the voters' roll once donors have withdrawn."[138] The result is that these (often expensive) technologies are then neither financially sustainable nor sufficiently safeguarded after donor support has ended. In our interviews we heard about cases of election technology "vendor lock-in," where countries had committed to expensive election technology, but were no longer able to maintain and update it without continued external support, and then struggled to switch to cheaper solutions due to dependencies on the original manufacturer. There were also cases where newly established digital databases containing parts of the civic registry had been endangered by shifts in political leadership,

134 Full Fact, "Full Fact AI," accessed January 4, 2024, https://fullfact.org/about/ai/.

135 Civil society representative, interview, October 5, 2023.

136 International IDEA, "ICTs in Elections Database," accessed May 24, 2024, https://www.idea.int/data-tools/data/icts-elections-database.

137 Nic Cheeseman, Gabrielle Lynch and Justin Willis, "Digital dilemmas: the unintended consequences of election technology," *Democratization*, 25, no. 8 (2015), p. 1397, https://doi.org/10.1080/13510347.2018.1470165.

138 Astrid Evrensel, "Introduction," in *Voter Registration in Africa: A Comparative Analysis*, ed. Astrid Evrensel, Johannesburg: EISA, 2010: pp. 1–56, https://www.eisa.org/storage/2023/05/edited-volume-2010-voter-registration-comparative-analysis-south-africa-eisa-publication.pdf.

where new leaders threatened to influence the registry to their advantage (e.g., to feed the database with "ghost voters").[139]

Technological solutions, then, risk being not only ineffective but dangerous: they give the impression of progress (sometimes at the cost of mismanaging voters' personal data and further eroding trust in the integrity of elections), but fail to grapple with the most important symptoms and manifestations of key digital risks that happen offline.[140] Instead, more successful efforts have focused on: identifying where tech can help implementers work more smoothly and impactfully; assessing the existing tech capacity of CSOs and intended beneficiaries; and ensuring that developing tech solutions does not create new gaps.[141] With a high level of investment, funders and implementing organizations have worked with local experts to identify the specific problems that tech could "fix." With a medium level of investment, donors have at least ensured there was the absorptive capacity within organizations (and the communities they target) to adopt tech "fixes." And with minimal investment (but a context-specific shift in what is considered "innovative"), donors have considered what lower-tech solutions they could get for the same level of investment, basing decisions on need rather than false assumptions about what tech offers.

●●● High Investment: Tailoring to the Tech Need

Funders and their project partners should work together with local experts to identify the specific problems that technology can fix. This is more likely to yield sensible applications of tech, aimed at creating solutions that will save time and scarce resources for implementers and CSOs. This was the focus for Full Fact, Africa Check, Chequeado, and the Open Data Institute when they won a grant from Google to use machine learning to improve and scale fact-checking. They collaborated with international experts to explore how artificial intelligence could transform this work. Drawing on their experience as fact-checkers, they have developed tools to address the most important needs that fact-checkers actually face: knowing the most important thing to be fact-checking each day; knowing when someone repeats something they already know to be false; and checking content in as close to real time as possible.[142]

The Google grantees intend to build a collaborative platform that will collect and monitor data; identify and label claims, and then match them with claims that have already been checked; and link to an external process that ensures the system remains relevant.[143] The project is still being rolled out, but it has already supported Nigerian fact-checkers in identifying false stories circulating around the 2023 election.[144]

Google has itself also been developing ways to support the work of fact-checkers in its operations. It has worked closely with the International Fact-Checkers Network to hone its search engine and help fact-checkers to better perform their work – such as through photo-dating technology, algorithms to highlight fact-checks when using the search function,

139 Donor official, briefing, May 24, 2024.

140 Rotmann and Watson, "Close the Gap: How to Leverage Local Analysis for Stabilization and Peacebuilding."

141 UNDP TfD, "Promoting Information Integrity in Elections: Global Reflections from Electoral Stakeholders," p. 15.

142 Full Fact, "Full Fact AI."

143 Ibid.

144 Kate Wilkinson, "Nigerian fact checkers fight election misinformation with Full Fact's AI Tools," *Google Blog*, February 20, 2023, accessed February 15, 2024, https://blog.google/intl/en-africa/company-news/technology/nigerian-fact-checkers-fight-election-misinformation-with-full-facts-ai-tools/.

or alert systems to flag debunked claims when they resurface.[145] While this is a laudable effort, it is important to note the criticism voiced about Google's complicity in the spread of disinformation on its platforms. Although it committed $300 million USD to supporting fact-checkers and journalists, a ProPublica investigation into the relationship between Google Ads revenue and election disinformation shows how the platform monetizes ads run on websites spreading disinformation, particularly in languages other than English. So, it is "that as one arm of Google helps support fact-checkers, its core ad business provides critical revenue that ensures the publication of falsehoods remains profitable."[146]

CSOs working in hostile environments, meanwhile, need tailored solutions to protect their online security. Several interviewees have identified a knowledge gap in accessing information and tools that could help organizations do their work online more safely. This insecurity can have huge implications for organizations' ability to run and to stay resilient against state parties (or other nefarious actors) hacking their accounts or tracking their activity – which potentially puts their programs at risk and their staff in physical danger. One organization we interviewed conducts digital security audits with the human rights organizations it works with; after these audits, it provides "fix-up" support to close identified gaps, for example by providing anti-virus software, Microsoft Office licenses or secure website hosting.[147]

Some interventions specifically work with the organizations and individuals most likely to be targeted by online attacks and hate speech. The Women@Web network, a DW Akademie-supported network of seven organizations in Kenya, Uganda, Tanzania, and Rwanda – Siasa Place, KICTAnet, The Launchpad, Media Convergency, Unwanted Witness, HerEmpire, and ABC Rwanda – has been working to combat online gender-based violence through research, peer-to-peer training and advocacy. It has particularly focused on women politicians, journalists and activists since 2018.[148] Similarly, Pollicy and the National Democratic Institute (NDI) Uganda target politicians or political aspirants across the political spectrum who are likely to be vulnerable to online violence, especially in the run-up to elections.[149] Their trainings often cover basic digital safety and literacy education, such as how to create safe passwords, use secure communication channels, engage with defamation and disinformation campaigns targeting them, and fact-check to prevent complacently sharing false information, as well as workshops on creative content and writing to engage different audiences. The Pollicy program Vote:Women consists of a fixed cohort of participants, who meet weekly online over the course of eight to ten weeks to use and improve their newly acquired digital skillset.[150] Similarly, we have seen other examples of capacity-building programs for women in tech, which consist of a fixed cohort meeting and learning together over a longer timeframe. One was designed to accompany women human rights defenders, activists, journalists, and media professionals through a mix of workshops, mentorship pairings, peer meetings, and self-guided trainings to strengthen their ability to secure themselves from digital incidents and harassment online.[151]

Positionality and marginalization play into individuals and organizations' vulnerability to digital threats and ability to safely engage online.

145 Ibid.

146 Craig Silverman, Ruth Talbot, Jeff Kao and Anna Klühspies, "How Google's Ad Business Funds Disinformation Around the World," *ProPublica*, October 29, 2022, accessed April 17, 2024, https://www.propublica.org/article/google-alphabet-ads-fund-disinformation-covid-elections.

147 Civil society representative, interview, October 13, 2023.

148 Johanna Rieß, "Women@Web: A regional network fights for women's digital rights," *DW Akademie*, October 30, 2020, accessed June 6, 2024, https://akademie.dw.com/en/womenweb-a-regional-network-fights-for-womens-digital-rights/a-55443823.

149 A. Kakande et al., "Byte Bullies: Understanding Violence against Women in Politics and Leadership - A study on the 2022 Kenya General Elections."

150 Irene Mwendwa and Rachel Magege (Pollicy), online interview, August 29, 2023.

151 Interview.

Not only do these programs show a deep understanding of existing capacities and needed interventions, but they also show the importance of understanding how positionality and marginalization may play into individuals and organizations' vulnerability to digital threats and ability to safely engage online. They address identified gaps through accessible, often continuous trainings, utilizing both online and offline approaches. Assessing existing needs for technology and actual gaps in human capacity is an essential guide to developing programming that responds to actual tech needs rather than desires for a "tech fix."

Medium Investment: Assess the Capacity to Use Tech

If such an assessment of the specific tech need is not possible, donors should at least assess that capacity of communities and CSOs to use the tech (or tech-based training) being provided. On the one hand, as already mentioned, the levels of internet penetration and digital literacy among potential partners are sometimes low. Interviewees explained that "some techniques to combat mis/dis/malinformation require a level of technical literacy that just isn't around, in addition to the difficulties of the lack of internet access."[152] On the other hand, many of the implementers, CSOs and other key stakeholders (like politicians and journalists) also operate in contexts where internet penetration is rapidly expanding; they, too, may be less digitally literate than international programmers would expect. For instance, in interviews some mentioned a dire need to improve the technological capacity of fact-checkers and journalists – including adequate training on how to use tools, such as VPNs, to protect themselves from surveillance.[153] This is why the digital security programs of DDP, CIPESA and others we spoke to include designated time for an organizational assessment of existing capacities. These assessments are essential to understand how organizations use technology both internally and in outward-facing communication, as well as where there are potential vulnerabilities.

Many organizations have struggled to get online at all in the face of prohibitive costs. One illustrative example of the type of restrictions citizens face is a tax introduced in Uganda in 2018, which charges citizens when they use social media platforms. Ostensibly meant to cut down on the spread of gossip, the tax is primarily aimed at creating another revenue stream for the government.[154] When the price of accessing the internet or social media services climbs for CSOs (who, as discussed, are often already facing financial challenges), it becomes increasingly difficult for them to maintain their audience reach or to access the online tools and training meant to support them. Among other digital security trainers, HerInternet – a Ugandan feminist organization promoting internet freedom and digital security for structurally marginalized and silenced women – mentioned the provision of data bundles for participants as an essential measure to enable participation in the face of potentially exclusionary data costs for a multiple-hour online training. Like the provision of circumvention technologies (VPNs), enabling data compensation can help make it possible for people to safely take part in the digital sphere.

152 Interview.

153 Enywaru Pius (PesaCheck), interview, Uganda, October 18, 2023.

154 Daniel Funke and Daniela Flamini, "A Guide to Anti-Misinformation Actions around the World," *Poynter*, accessed July 27, 2023, https://www.poynter.org/ifcn/anti-misinformation-actions/.

Minimal Investment: Consider Lower-Tech Solutions

In tackling digital threats that take advantage of societal mistrust or media illiteracy, it is very probable that the most useful solutions will not be based in AI or machine learning but will be tried-and-tested techniques aimed at social cohesion, building trust in media institutions, educating the public, or training and accompanying organizations. It is essential that international organizations continue to consider these approaches, to ensure that the criterion for programming is what will be most effective, not what seems more technologically advanced.

Ensure that the criterion for programming is what will be most effective, not what seems more technologically advanced.

Interviewees consistently highlighted that the most useful "tech solutions" were often basic skill trainings. In fact, getting organizations or political changemakers online and teaching them how to effectively use social media for their work (e.g., to reach new audiences or amplify their advocacy) is often a first step before introducing more advanced technological solutions.[155] DDP also provides funds for digital security-related technologies like VPNs, and – to mitigate digital work-related stressors – training and holistic support services including therapy, counseling and group therapy.[156] Before (or even instead) of opting for more advanced technical interventions, these types of efforts help foster safer and more knowledgeable online engagement.

Similarly, in-person approaches often prove more useful in addressing the dangers of mis-and disinformation or hate speech and in fostering media literacy. This is especially true when engaging with communities that favor or trust traditional media over digital sources, or with communities that have a low internet penetration rate due to prohibitive connectivity costs or insufficient internet infrastructure in their region. An example of an in-person approach helping bridge the gap between online space and its offline implications is the community dialogue format developed by the Human Rights Network for Journalists Uganda (HRNJ-Uganda). The community dialogue's goal is to improve trust in quality journalism and help journalists better respond to the communities they report on. At these in-person convenings, facilitated by HRNJ-Uganda, the public can share grievances with the media houses and journalists that come into their communities to report – and vice versa. This exchange is accompanied by explanations of how journalists operate and what communities can and cannot expect from them.

To take another example, Media Focus on Africa Uganda has organized community dialogues with their partners to facilitate discussions on election promises and accountability strategies. These dialogues aim to improve journalist—community relationships and empower the public to push the media to hold politicians accountable.[157] Several of the media organizations we interviewed identified a need for public-centered journalism programs that create a sense of personal connection between communities and "their" journalists.[158] The theory of change for this work is that once journalists are perceived as "part of society," community members are more likely to disagree with (and at times even actively speak out against) the repression of journalists in their community. The same level of trust is unlikely to be built by technological or online solutions.

155 International organization representative, interview, Uganda, October 13, 2023; Irene Mwendwa and Rachel Magege (Pollicy), online interview, August 29, 2023.

156 Digital Defenders Partnership (DDP) representative, online interview, July 25, 2023.

157 Civil society representative, interview, Uganda, October 19, 2023.

158 HRNJ-Uganda representative, interview, Uganda, October 18, 2023, and online interview, November 2, 2023; DW Akademie Uganda representative, interview, Uganda, October 17, 2023.

DW Akademie Uganda takes a congruent approach with its Uplifting Community Voices project, which has been running since 2015 and aims to improve public service delivery reporting and strengthen Uganda's highly localized media structures over the long term. The program works with rural media houses to enable journalists to report on hyperlocal stories in remote locations, which would otherwise be unprofitable due to high travel costs. Uplifting Community Voices employs community reporters that were identified by the media houses, endorsed by the community as trusted members, and trained by DW Akademie Uganda. This allows the program to create a sense of local ownership and strengthen ties between communities and their local journalists and news stations, since hyperlocal news is much more relevant to their daily lives than reporting exclusively focused on big cities. Interviewees reported that previously, when governments clamped down on radio stations during elections, listeners used to keep quiet because radio shows were not broadcasting anything of relevance to them. But now, hyperlocal reporting and the use of community reporters have contributed to the shared sense that "this is our radio" – and to a greater willingness to put pressure on officials.[159] Beyond individual reporters, the project also supports partner media houses with their institutional capacity and business models, thus helping a diverse and sustainable independent media landscape remain viable in Uganda.

When the CSO community is forced to move offline, these lower-tech solutions become more important than ever. A number of organizations – such as Access Now and DDP – have provided training and guidebooks to help CSOs navigate the sudden loss of connectivity. Access Now developed the *Internet Shutdowns and Elections Handbook*, which "provides tips and recommendations for key actors to navigate shutdowns and understand and assess the extent to which an election taking place under a shutdown is free and fair."[160] Similarly, another CSO we interviewed delivers internet shutdown trainings for partner CSOs and journalists who monitor access to information during elections, which includes training on how to measure the effect of shutdowns as well as the provision of VPNs and other software. These lower-tech tools are essential for organizations to be able to quickly adapt to internet restrictions.

Experts have also emphasized the importance of allowing partners to use funds to ensure the physical, offline safety of their staff, partners and workspaces.[161] For instance, DDP provides funds for physical security that includes necessary devices, such as CCTV cameras for offices. One interviewee also mentioned a temporary relocation program for human rights defenders that operates across the African continent. The program includes a support component where CSOs local to the host city help the newcomers find their footing and develop coping mechanisms for the threats they faced. A micro-grants fund is also part of the relocation program, allowing these human rights defenders – who include journalists, lawyers, activists, and artists facing threats due to their work online – to cover relocation costs, legal fees or costs to replace devices. Considering lower-tech solutions, then, means recognizing the offline consequences of online work and, like this relocation program, working to bridge digital and physical security while making it possible for beneficiaries to continue their work.

159 DW Akademie Uganda representative, interview, Uganda, October 17, 2023.

160 Access Now, "Internet Shutdowns and Elections Handbook."

161 Digital Defenders Partnership (DDP), online interview, July 25, 2023.

Conclusion: Strategic Direction Needed for Change

The risks of digital threats to elections in Africa are increasing. Citizens can more cheaply and easily transcend country borders via the internet, and many systems around elections are being digitized with the promise of improving government effectiveness and transparency. Unfortunately, the same online spaces are being exploited by those seeking to silence dissent and erode democratic institutions. Many interviewees spoke with frustration about fruitless conversations with tech companies unwilling to quickly respond to harmful content on their platforms. Human rights defenders are still worried about the next internet shutdown in their country, which would inevitably bring their activities grinding to a halt. And in the meantime, many fear that limited resources and their governments' increasing authoritarian tendencies will force them to shut their doors anyway.

Experts all over the world – not just in Africa – are ever more concerned about the increasing sophistication of deepfakes and the difficulty of stopping dangerous lies from spreading online. As one commentator notes, generative AI is enabling untold numbers of people to spread disinformation "by making it simple, cheap and more convincing."[162] It is, then, crucial that democracy supporters learn from past successes and mistakes alike as they develop smart responses to digital threats to elections around the globe. Many countries have also placed advances in technology at the forefront of their foreign policies.[163] The Africa Election Fund, launched by UNDP and Germany in 2023, describes one of its aims to be "address[ing] how rapid technological evolution offers the potential for greater inclusion of citizens, but equally increases the pace of unverified or inaccurate information sharing, impacting trust in media and democratic processes."[164] The EU's recently passed AI Act also "aims to protect fundamental rights, democracy, the rule of law and environmental sustainability from high-risk AI" within its member states.[165] The African Union has also been at the forefront of calling for a freer, fairer and safer internet;[166] for instance, ahead of this year's slate of elections, it tasked African states with ensuring "secure internet before, during and after elections."[167] This indicates the significant interest in improving international and regional responses to advances in technology, including during election times.

It is crucial that democracy supporters learn from past successes and mistakes alike as they develop smart responses to digital threats to elections.

The welcome attention to digital threats to elections must, however, be combined with better efforts to address such threats. But better does not mean simply funding more activities;

162 Helen Fitzwilliam, "How AI Could Sway Voters in 2024's Big Elections," *Chatham House*, September 29, 2023, accessed June 6, 2024, https://www.chathamhouse.org/publications/the-world-today/2023-10/how-ai-could-sway-voters-2024s-big-elections.

163 See, e.g., The White House, "Fact Sheet: Advancing Technology for Democracy," March 29, 2023, accessed June 6, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad.

164 UNDP, "Germany and UNDP launch the Africa Election Fund to support electoral processes in Africa."

165 European External Action Service (EEAS), "The EU's approach to artificial intelligence centres on excellence and trust," April 23, 2024, accessed June 6, 2024, https://www.eeas.europa.eu/delegations/united-kingdom/eu%E2%80%99s-approach-artificial-intelligence-centres-excellence-and-trust_en.

166 African Union, "The Digital Transformation Strategy for Africa (2020-2030)," May 18, 2020, accessed June 6, 2024, https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030; AUDA-NEPAD, "AI for Africa: Artificial Intelligence for Africa's Socio-Economic Development," *African Union Development Agency*, August 2021, accessed June 6, 2024, https://www.nepad.org/publication/ai-africa-artificial-intelligence-africas-socio-economic-development.

167 African Commission on Human and Peoples' Rights, "Resolution on Internet Shutdowns and Elections in Africa."

instead, as discussed throughout the report, it is paramount to invest in and commit to more knowledge-led, context-specific and collaborative efforts to tackle digital threats. This applies both on a programmatic and a diplomatic level. This report, then, sought to understand how efforts to tackle digital threats can be improved across four areas that require change, and examine how varying levels of investment can unlock effectiveness in each one:

Understanding the digital threat landscape: More successful efforts have used baseline surveys, iterative learning and post-program reviews to ensure that funding is aimed at real need, instead of relying on flawed assumptions about the most pressing issues or most useful responses. In doing so, organizations have been able to tailor their programs to needs identified ahead of the project start, better adapt interventions based on continuous learning throughout the project, and understand and evaluate the impact of their measures after they have been implemented.

Varied actors for varied digital threats: More successful efforts have brought together a variety of stakeholders (through coalitions, strategic coordination and facilitated networking) and developed multi-pronged solutions to a diverse range of threats. Coalition-building and coordination were used to collectively advocate against internet shutdowns, strategically cooperate in mitigating dis- and misinformation around elections, and strengthen political commitments to an open digital space.

Taking an institutional approach to digital threats: More successful efforts committed funding to address organizational gaps through (albeit limited) co-designing of projects, organization-wide training and filling core institutional capacity gaps. These approaches helped to address the broader structural issues many organizations face. Successful examples opted for several month-long organizational accompaniment programs, funded core support instead of only resourcing another project, and entered into direct partnerships with local organizations.

Hybrid solutions for hybrid problems: More successful efforts were able to develop more appropriate (and often much lower-tech) solutions by prioritizing approaches that were not purely online, and by focusing on understanding the actual technological needs and assessing the capacity of CSOs and their target audiences. In doing so, organizations were able to identify potential solutions to address human gaps in fact-checking; invest resources in face-to-face community dialogues; address communities' media literacy shortfalls; and provide mentorship and training to those, like women politicians, who are most likely to face digital violence.

The digital threats discussed here are not unique to Africa. While specific challenges may differ across contexts, the resourceful approaches highlighted in this report – as well as the building blocks to guide interventions – are relevant to the many places across the globe where digital threats undercut democratic norms, exacerbate social polarization and aggravate existing marginalization. This report hopes to have provided some insight into how others have attempted to tackle these threats. In doing so, it has sought to give guidance to officials, experts and practitioners in national governments, international organizations and CSOs who hope to address digital threats to elections in the myriad ways they manifest, both on- and offline.

Appendix 1: Further Reading

We spoke to many organizations working in and on Africa (as well as some that work globally) who have already contributed important guides, databases, educational games, toolkits, and reports to tackling digital threats to elections in Africa. To help those seeking to understand the work already being done, below we have collected some of the work we have drawn on and referenced throughout the report. While this is not an exhaustive list, it may serve as a useful starting point.

Databases

- **Tech for Good:** Civic Tech Field Guide is a collection of projects around the world using tech for the common good. Can be accessed here: https://civictech.guide/.
- **Online Freedom:** Freedom House's "Freedom on the Net" (annual survey and analysis of internet freedom around the world) and "Election Watch for the Digital Age" (tracking elections and the digital sphere). Can be accessed here: https://freedomhouse.org/report/freedom-net; https://freedomhouse.org/report/election-watch-digital-age.
- **Online Freedom:** LEXOTA provides detailed analysis on laws and government actions on disinformation across sub-Saharan Africa. Can be accessed here: https://lexota.org/about-page/.
- **Internet Shutdowns:** Access Now's 2024 Elections and Internet Shutdowns Watch is a watchlist of elections scheduled for 2024 where a high risk for internet shutdowns was identified. The list of internet disruption incidents is regularly updated and can be accessed here: https://www.accessnow.org/campaign/2024-elections-and-internet-shutdowns-watch/.
- **Internet Shutdowns:** Internet Society Pulse consolidates trusted third-party internet measurement data from various sources into a single platform. Can be accessed here: https://pulse.internetsociety.org/.
- **Access to Information:** "Access to Information Laws in Africa." Collection of reports by the Africa Freedom of Information Center. Can be accessed here: https://www.africafoicentre.org/foi-laws/.

Online Games

- **Digital Safety:** "Ayeta: A proactive toolkit for African digital rights actors," by Paradigm Initiative. Can be accessed here: https://paradigmhq.org/programs/digital-rights/ayeta/.
- **Digital Safety:** "Digital SafeTea," by Pollicy. Can be accessed here: https://pollicy.org/projects/digital-safetea/.
- **Mis- and Disinformation:** "Choose Your Own Fake News," by Pollicy. Can be accessed here: https://pollicy.org/projects/choose-your-own-fake-news/.

- **Mis- and Disinformation:** "Get it Right," by Digital Public Square and the International Centre for Investigative Reporting Nigeria. Can be accessed here: https://getitrightnigeria.com/.

Africa-Wide Networks

- **Digital Rights:** The African Internet Rights Alliance (AIRA) is a network of Africa-based civil society organizations that advance digital rights. Details can be found here: https://aira.africa/.
- **Digital Rights:** The African Digital Rights Network (ADRN) is a network of activists, academics and analysts who carry out research on digital rights in Africa. Details can be found here: https://www.africandigitalrightsnetwork.org/.
- **Online Freedom:** African Freedom of Expression Exchange (AFEX) is the African chapter of IFEX, a global network over 100 organization working on freedom of information and expression. The AFEX network convenes African organizations working on freedom of expression and media rights. Details can be found here: https://www.africafex.org/.
- **Media Freedom:** Media Institute of Southern Africa (MISA) has chapters in 11 countries in Southern Africa and works on promoting media freedom, freedom of expression and access to information. Details can be found here: https://misa.org/.

International Networks

- **Online Freedom:** The Freedom Online Coalition convenes 39 governments, working to advance internet freedom through knowledge sharing, diplomatic coordination and advocacy. Details can be found here: https://freedomonlinecoalition.com/.
- **Online Freedom:** IFEX is a global network of organizations promoting and fighting for freedom of expression. Details can be found here: https://ifex.org/.
- **Internet Shutdowns:** Access Now's #KeepItOn coalition consists of more than 300 organizations across the globe fighting to end internet shutdowns. Details can be found here: https://www.accessnow.org/issue/internet-shutdowns/.
- **Mis- and Disinformation:** International Fact-Checking Network (IFCN) at Poynter. Details can be found here: https://www.poynter.org/ifcn/.
- **Information Integrity:** The Action Coalition on Information Integrity in Elections is convened by UNDP with the support of the Danish Government's Tech4Democracy Initiative. Details can be found here: https://www.undp.org/policy-centre/governance/projects/action-coalition-information-integrity-elections.

Practitioner Guides and Further Reading

- **Online Freedom:** "Examining the Effect of Shrinking Civic Space on Feminist Organizing Online, Particularly for Structurally Silenced Women in Uganda" (2021), by Women of Uganda Network (WOUGNET) and Association for Progressive Communications (APC). Can be accessed here: https://wougnet.org/download/examining-the-effect-of-shrinking-civic-space-on-feminist-organizing-online-particularly-for-structurally-silenced-women-in-uganda/.

- **Digital Security:** "Digital Safety Manual for Diplomats," by Digital Defenders Partnership, contains information and tips on enhancing digital security for embassy staff working with civil society and human rights defenders. Can be accessed here: https://digitalsafetymanual.org/.

- **Digital Threats:** "Tech Harms During Elections in Africa" (2024), by Bulanda T. Nkhowani of Digital Action, as part of the Global Coalition for Tech Justice. Can be accessed here: https://yearofdemocracy.org/tech-harms-during-elections-in-africa/.

- **Mis- and Disinformation:** Information Integrity for Electoral Institutions and Processes Reference Manual for UNDP Practitioners (2024). Can be accessed here: https://www.undp.org/policy-centre/governance/publications/information-integrity-electoral-institutions-and-processes-reference-manual-undp-practitioners.

- **Mis- and Disinformation:** "Protecting Electoral Integrity in the Digital Age: The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age" (2020). Can be accessed here: https://www.kofiannanfoundation.org/supporting-democracy-and-elections-with-integrity/safeguarding-the-legitimacy-of-elections-the-kofi-annan-commission-launches-final-report/.

- **Mis- and Disinformation:** "Protecting Democratic Elections through Safeguarding Information Integrity" (2024), by Democracy Reporting International, Forum on Information & Democracy and International Institute for Democracy and Electoral Assistance. Can be accessed here: https://www.idea.int/publications/catalogue/protecting-democratic-elections-through-safeguarding-information-integrity.

- **Mis- and Disinformation:** "Social Media Hate Speech Mitigation Field Guide" for Ethiopia (2020), Cameroon (2021) and South Sudan (2018), by #Defyhatenow. The interactive Ethiopia field guide can be accessed here: https://defyhatenow.org/defyhatenow-field-guide-ethiopia/. The Cameroon field guide can be accessed here: https://defyhatenow.org/cameroon/social-media-hate-speech-mitigation-field-guide-v2-cameroon/. The South Sudan field guide can be accessed here: https://defyhatenow.org/social-media-hate-speech-mitigation-field-guide/.

- **Mis- and Disinformation:** "Detoxing information ecosystems: A proactive strategy for tackling disinformation" (2024), by Steffen Leidel and Dennis Reineck, published by DW Akademie. Can be accessed here: https://akademie.dw.com/en/detoxing-information-ecosystems-a-proactive-strategy-for-tackling-disinformation/a-68820226.

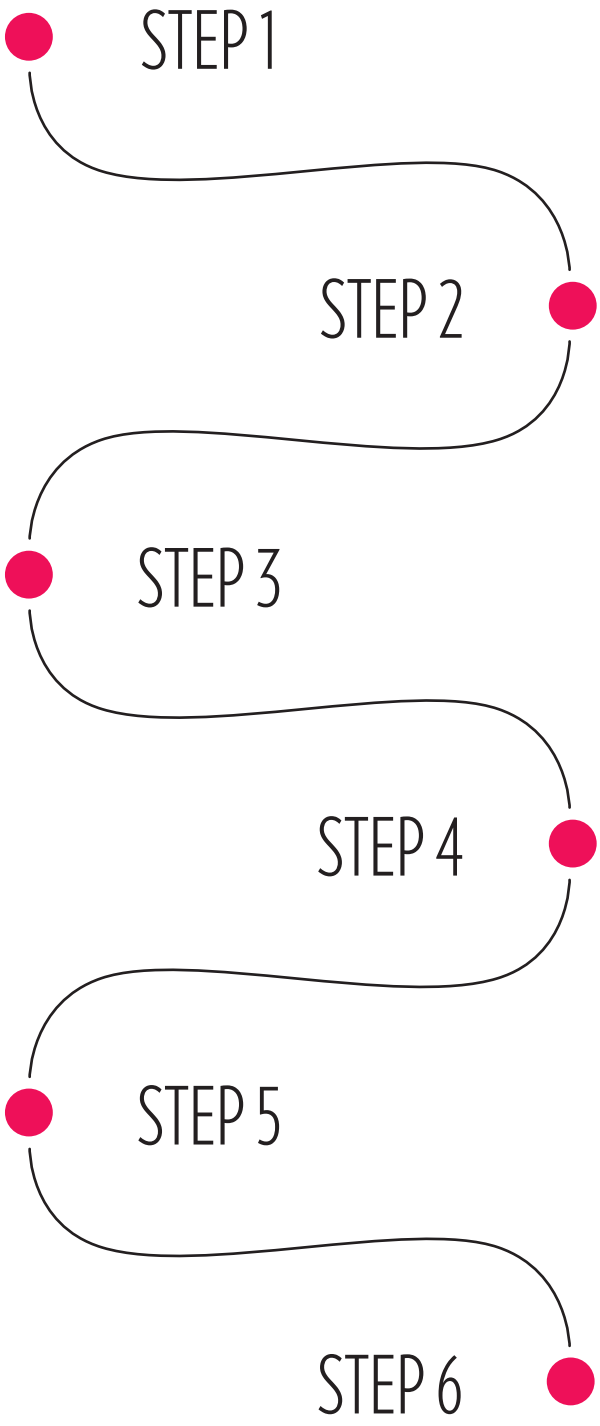
- **Mis- and Disinformation:** "A Tapestry of Actors, Attitudes, and Impact: Countering Disinformation in Africa" (2024) by Juliet Nanfuka, Victor Kapiyo, Victor Mabutho, Wairagala Wakabi PhD, published by Bertelsmann Stiftung. Can be accessed here: https://www.bertelsmann-stiftung.de/en/publications/publication/did/a-tapestry-of-actors-attitudes-and-impact-countering-disinformation-in-africa.

- **Internet Shutdowns:** "Internet shutdowns and elections handbook: A guide for election observers, embassies, activists, and journalists" (2021), by Access Now. Can be accessed here: https://www.accessnow.org/guide/internet-shutdowns-and-elections-handbook/.

- **Internet Shutdowns:** "Advancing Strategic Litigation on Internet Shutdowns Cases in Africa: Promises and Pitfalls," by Dunia Mekonnen Tegegn, published by CIPESA. Can be accessed here: https://cipesa.org/wp-content/files/Advancing-Strategic-Litigation-on-Internet-Shutdowns-cases-in-Africa-Promises-and-Pitfalls.pdf.

- **Information Integrity:** "Defending Information Integrity: Actions for Election Stakeholders" (2024), by the United Nations Development Programme's Global Policy Centre for Governance. Can be accessed here: https://www.undp.org/policy-centre/governance/publications/defending-information-integrity-actions-election-stakeholders.

Appendix 2: Creating Scenarios for the 2024 Elections in Ghana and Mozambique



Scoping

Decide on scenario topic and the purpose of the scenario process (e.g. creating different threat scenarios to underscore the potential variety and combinations of threats to elections).

Identifying key factors

Topic experts name and describe all relevant factors expected to shape the electoral process, its integrity and the potential for electoral violence.

Analyzing key factors

Consolidate key factors, then topic experts assess each factor in terms of uncertainty and impact and create descriptive projections for how each could play out.

Building scenario frameworks

Create different combinations of the projections from Step 3 to construct unique scenarios.

Transferring scenarios

Develop a short narrative for each scenario, explaining how the different combinations of projections connect with each other to produce the given outcome.

Using the scenarios for stress testing

Develop programming strategies to mitigate the key threats in each scenario, and collaborate (e.g., in a workshop) to test their efficacy across scenarios.

This overview sketches the steps we took to develop scenarios for a strategic foresight workshop in which funders, experts and implementers "gamed" possible strategies that external democracy supporters could implement to counter the relevant digital threats to two specific elections. Scenarios were used to help participants understand the context in which digital threats emerge, identify and diversify current assumptions about the future, and discuss how to adapt future programming.[168] The examples used were the 2024 elections in Ghana (scheduled for December 7, 2024) and Mozambique (scheduled for October 9, 2024). Scenario construction took place across a series of expert surveys and analysis by GPPi over the course of several months between December 2023 and April 2024.

The two scenario case studies were chosen based on their likeliness to see international donor engagement and their diverging contexts (which will require very different policy and programming responses), as well as their timing in the second half of 2024. In Ghana's upcoming presidential election, there is likely to be a democratic handover of power despite potential manipulation attempts, and online mis- and disinformation will play an important role given the country's relatively high connectivity rates and the prevalence of dis-and misinformation in previous elections.[169] In Mozambique, election results will be manipulated (as one workshop participant said, "it is just a matter of how rigged"), and the limited connectivity in the country means that digital threats will have a far less pivotal role, though internet shutdowns are perceived to be more likely than in Ghana.[170]

Step 1: Scoping – What Do We Want to Build Scenarios For?

We decided to focus on creating different threat *scenarios*[171] for each country to underscore the potential variety and combinations of threats to the integrity of elections and the risks of electoral violence.[172] We also decided that our scenarios would cover a time period that included the run-up to the election, election day, and the post-election period before the next government would take office. To ensure a diversity of perspectives – including experts from and based inside the country in question, as well as experts living abroad; interdisciplinary perspectives on the elections; and a variety in gender and age – we sought to include 10–20 experts per country in the exercise. In the end, 14 experts participated for Ghana and 11 did for Mozambique.

168 For more details on foresight methodologies, see Sarah Bressan and Philipp Rotmann, "Looking Ahead: Foresight for Crisis Prevention," July 3, 2019, accessed June 19, 2024, https://gppi.net/2019/07/24/looking-ahead-foresight-for-crisis-prevention.

169 Gabrielle Lynch, Elena Gadjanova and Ghadafi Saibu, "The hidden costs of social media use in elections: A Ghana case study," *The Conversation*, December 3, 2019, accessed June 6, 2024, https://theconversation.com/the-hidden-costs-of-social-media-use-in-elections-a-ghana-case-study-128007; Joseph Siegle and Candace Cook, "Africa's 2024 Elections: Challenges and Opportunities to Regain Democratic Momentum," *Africa Center for Strategic Studies*, January 17, 2024, accessed June 6, 2024, https://africacenter.org/spotlight/2024-elections/.

170 Africa Center for Strategic Studies, "Mozambique: October 9," January 17, 2024, accessed June 6, 2024, https://africacenter.org/spotlight/2024-elections/mozambique/; Dércio Tsandzana, "Mozambique: Digital landscape and internet disruption in the context of elections," Global Voices, December 28, 2023, accessed June 6, 2023, https://globalvoices.org/2023/12/28/mozambique-digital-landscape-and-internet-disruption-in-the-context-of-elections/; Zach Rosson, Felicia Anthonio and Carolyn Tackett, "Shrinking Democracy, Growing Violence: Internet shutdowns in 2023," *Access Now*, May 2024, accessed May 15, 2024, https://www.accessnow.org/internet-shutdowns-2023/.

171 Italicized terms are taken from foresight methodologies. For further reading, see Bressan, Nygård and Seefeldt, "Forecasting and foresight: Methods for anticipating governance breakdown and violent conflict."

172 Ibid., p. 16.

Step 2: Identifying Key Factors

In a first closed survey, expert participants were asked to name and describe all relevant *factors* they expected would shape the electoral process, its integrity and the emergence of electoral violence.

- **Ghana:** participants provided 96 factor suggestions with descriptions
- **Mozambique:** participants provided 85 suggestions with descriptions

The project team clustered the factors, combining redundant and very similar suggestions into a smaller number of mutually exclusive and collectively exhaustive final factors, with detailed and intersubjectively plausible descriptions.

- **Ghana:** 22 final factors
- **Mozambique:** 25 final factors

Step 3: Analyzing Key Factors[173]

In a second closed survey, the same expert participants were given the list of final factors for their assigned country. They then rated each one in terms of its uncertainty and potential impact. Based on the expert ratings, the project team completed an uncertainty—impact analysis that identified a small number of particularly relevant factors. These factors are referred to as *key uncertainties*.

The participants were also asked to provide several *projections* for a number of factors. The projections aimed to describe different (again mutually exclusive) ways that each factor might play out in the scenario period.

- **Ghana:** participants provided 310 individual projections
- **Mozambique:** participants provided 232 individual projections

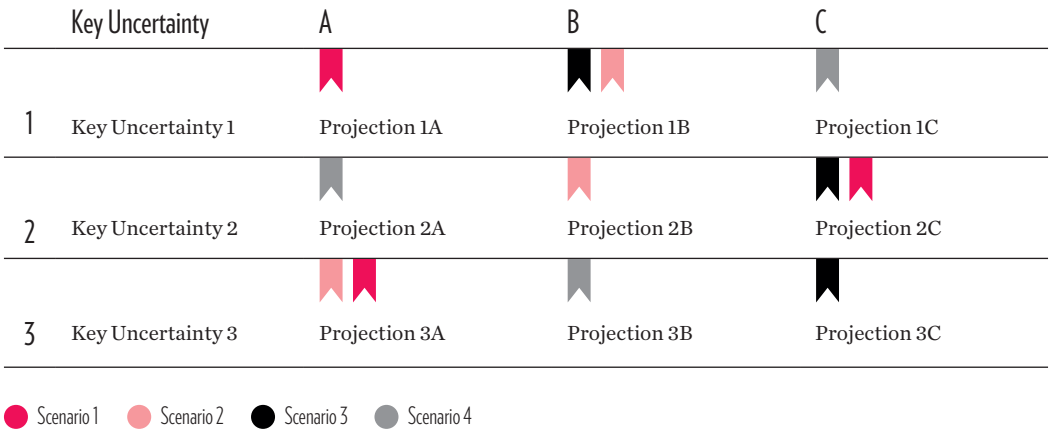
The experts' projections, again clustered from many submissions into a more manageable set of two-to-four diverging projections per key uncertainty, became the building blocks of our scenarios. See Figure 1 below, which offers an abstracted overview of how key uncertainties and projections combine into a *scenario framework*.

Example projections for a key uncertainty from Ghana, named "Impact of mis/disinformation": (1A) mis/disinformation is successfully debunked; (1B) it proliferates significantly and shapes election results; and (1C) it is less impactful due to the closeness of the election.

Example projections for a key uncertainty from Mozambique, named "Impact of poverty and inequality": (1A) people disengage and do not vote; (1B) people protest; and (1C) hardship drives votes for the opposition.

173 Ibid., p. 18.

Figure 1: Key Uncertainties and The Three Diverging Projections For Each



Step 4: Building Scenario Frameworks[174]

The project team then combined divergent projections for the key uncertainties into distinct scenario frameworks. Each framework drew one projection from each of the key uncertainties, which together defined what happens in a given scenario. For each country, three scenario frameworks were created.

Figure 2: The Diverging Projections Being Grouped Together To Form Different Scenarios

Scenario 1	Scenario 2	Scenario 3	Scenario 4
Projection 1A	Projection 1B	Projection 1B	Projection 1C
Projection 2C	Projection 2B	Projection 2C	Projection 2A
Projection 3A	Projection 3A	Projection 3C	Projection 3B

Step 5: Transferring Scenarios[175]

For each of the three scenario frameworks per country, the team developed a short narrative to create a "*history of the future*," explaining how events could unfold given that framework's particular set of uncertain and impactful factors.[176]

The narrative scenarios were presented at the in-person strategic foresight workshop. To help the expert participants immerse themselves in the scenarios, the narratives were supported by elements like fictional newspaper snippets or social media posts, which helped illustrate the key dynamics driving each scenario, as well as its consequences for the subject of our analysis: the integrity of the election and the risk of electoral violence.

174 Bressan, Nygård and Seefeldt, "Forecasting and foresight," p. 19.

175 Ibid, p. 20.

176 Ibid., p. 20.

At the workshop, the expert participants – some of whom had been part of the scenario construction surveys – worked through the scenarios and made additional tweaks to ensure plausibility while retaining three distinct scenarios for each country.

Step 6: Using the Scenarios for Stress Testing

The resulting scenarios formed the environment for stress testing programming strategies,[177] which aimed to mitigate the key threats in each scenario.

177 U.K. Gov, "The Futures Toolkit," accessed May 29, 2024, https://assets.publishing.service.gov.uk/media/5a821fdee5274a2e8ab579ef/futures-toolkit-edition-1.pdf.

Acknowledgments

We would like to thank everyone who throughout the past year and a half, helped shape the project on which this publication is based. At the German Federal Foreign Office, we are particularly thankful for the close collaboration with Klemens Semtner, Sonja Riemer and Lieneh Modalal, whose engagement and openness was instrumental for the entire effort.

We benefitted from the many experts and practitioners who gave up their time to speak to us, attend workshops, review drafts, and share relevant information. These include: Admire Mare (Department of Communication and Media Studies, University of Johannesburg), Alasdair Stuart (BBC Media Action), Anita R. Gohdes (Hertie School), Anna Bwana (BBC Media Action Tanzania), Ashnah Kalemera (CIPESA), Gilbert Sendugwa (AFIC), Jamie Hitchen, Juliet Nanfuka (CIPESA), Jonathan Fisher (University of Birmingham), Joshua Kitili (Centre for Intellectual Property and Information Technology Law), Magambo Emmanuel (HRNJ-Uganda), Marystella A. Simiyu (Centre for Human Rights, University of Pretoria), Nompilo Simanje (International Press Institute), Rachel Magege (Pollicy), Sandra Aceng (WOUGNET), and Shujazz. Some of the experts we spoke to have chosen to remain anonymous; we also thank them. None of these individuals bear any responsibility for mistakes in the report.

We would also like to thank our GPPi colleagues Gelila Enbaye, Wade Hoxtell, Philipp Rotmann, and Thorsten Benner for providing valuable feedback on earlier drafts. Ayşe Lara Selçuker and Maximilian Biller helped lay important conceptual and empirical foundations for this project during their internships at GPPi. Finally, we would like to thank Sonya Sugrobova, Marc Shkurovich and Katharina Nachbar for their excellent editorial work and their creative input on this project.

This publication is funded by the German Federal Foreign Office as part of the project "Stabilization Lab: Improving Key Instruments for Crisis Prevention, Conflict Resolution and Peacebuilding." The views expressed herein solely reflect those of the authors and do not present the official position of the German government.

Reflect. Advise. Engage.

The Global Public Policy Institute (GPPi) is an independent non-profit think tank based in Berlin. Our mission is to improve global governance through research, policy advice and debate.

Cover Photo: Shutterstock/Tolu Owoeye

Reinhardtstr. 7, 10117 Berlin, Germany
Phone +49 30 275 959 75-0
gppi@gppi.net
gppi.net