Shutting Down the Shutdown

Mainstreaming Proactive Civil Society Responses to Internet Disruptions

INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

Shutting Down the Shutdown
Mainstreaming Proactive Civil Society Responses to Internet Disruptions

Please send all requests for permission to:
Attn: Department of External Affairs
International Republican Institute
1225 Eye Street NW, Suite 800
Washington, DC 20005
info@iri.org

About Us | The International Republican Institute (IRI)

A nonprofit, nonpartisan organization, the International Republican Institute (IRI) advances freedom and democracy worldwide by helping political parties become more responsive, strengthening transparent and accountable governance, and working to increase the role of marginalized groups in the political process—including women and youth. Since 1983, IRI has supported civil society organizations, journalists, and democratic activists – in Africa, Asia, Eurasia, Europe, Latin America and the Caribbean, the Middle East and North Africa – with programs in over 100 countries. IRI's Technology & Democracy Practice promotes digital democracy, civic and government technology, internet freedom, and information integrity in every region of the world. In addition to critical internet freedom technologies, IRI works to mainstream internet freedom tools into democracy, rights, and governance programming to increase knowledge and access to these tools for activists, independent media, civil society organizations (CSOs) and other democracy partners, especially those in repressive environments.

Acknowledgments

This report was written by Josh Willard.

We thank the many individuals from around the world who supported IRI in the development of this report, including for their contributions as working group members and reviewers. We thank Nat Kretchun, Eman Jaradat, Sarah Moulton, Zach Rosson, Felicia Anthonio, Ben Whitehead, Laura Schwartz-Henderson, Bryan Nunez, Sameer Syed, Scott Carpenter, Justin Henck, Vinicius Fortuna, Grace Kwak Danciu, and Tawanda Mugari for sharing the real-world expertise that made this report possible. We would also like to thank Diana Kurth, Katie Harbath, and Maura McCrary for their support in standing up the working group. Thanks to Hui Hui Ooi and Jared Ford for their feedback, guidance, and leadership.

We also thank Google Jigsaw for its support of the Internet Freedom Working Group.

Finally, we would like to acknowledge our peers and partners in the internet freedom community for their tireless work to identify, research, and condemn internet shutdowns whenever and wherever they occur. In particular, we would like to acknowledge our working group partners Internews and Access Now for their leadership and expertise on the subject of internet shutdowns. Research published by Internews' OPTIMA program, Access Now, and the #KeepItOn coalition proved invaluable to this report.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Internet shutdowns threaten the fundamental human rights of billions of people. Yet, most civil society organizations and activists remain unprepared to mitigate the threat. Without a response plan, authoritarians[1] can effectively obstruct the flow of information to and from civil society organizations. While a growing international coalition is working to address the threat of internet shutdowns head on, the issue persists.

A more proactive, cross-sectoral response is needed. In this report, IRI and its partners in the Internet Freedom Working Group (IFWG) urge stakeholders across the democracy, rights, and governance (DRG) community to join the internet freedom community by encouraging proactive civil society responses to internet shutdowns.

The recommendations contained in this report are a call to action—for DRG implementers, funders, policymakers, and internet freedom tool developers—to take tangible steps to prepare for internet shutdowns. Whole-of-society preparedness is the only sustainable approach to a whole-of-society problem like internet shutdowns. To be clear, every human rights defender does not need to become a tech expert.

However, the scale and frequency of internet shutdowns mean that no human rights defender can afford to ignore the threat of internet shutdowns. Steps by actors on the ground, enabled by the key stakeholders outlined below, can be the difference between connecting when it matters most or being left in the dark.

To help prepare for internet shutdowns:

DRG implementers should...

- Set up coordination channels to share resources with local partners.
- Help local partners create their own Internet Freedom Preparedness Plan.
- Train program staff on internet shutdown preparedness.
- Mainstream internet shutdown preparedness beyond internet freedom programming.
- Plan for internet shutdowns in advance of elections.

Funders should...

- Require grantees to have an Internet Shutdown Preparedness Plan.
- Mandate quarterly risk assessments.
- Reward information sharing.
- Provide rapid-response funding.
- Incentivize mass deployment of internet freedom tools in smaller countries.

Policymakers should...

- Build proactive programming to prepare for internet shutdowns into foreign assistance funding.
- Clarify internet freedom exceptions in sanctions.
- Consult with technologists throughout the sanctions process.

And technologists should...

- Improve the measurement of internet shutdowns.
- Consult with frontline users during tool development.
- Prioritize the localization of existing tools.
- Workshop translation and localization challenges.
- Prioritize open-source components.

[1] A note on word choice: Internet shutdowns have occurred in autocratic, hybrid, or democratic countries. For the purposes of this report, we refer to the perpetrators of internet shutdowns simply as authoritarians, because the desire to silence dissent (i.e., the driver of internet shutdowns) is a fundamentally anti-democratic impulse, regardless of the political system in which the perpetrator operates.

INTRODUCTION: WHY WE WROTE THIS REPORT

IRI wrote this report to share the findings of the Internet Freedom Working Group with the public, especially those actors who work to advance human rights and democracy but have not mainstreamed internet shutdown preparedness into their programming. IRI hopes that DRG implementers (IRI included), funders, policymakers, and technologists can apply the recommendations herein to help civil society organizations (CSOs) and individuals better prepare for internet shutdowns before they occur.

The report is intended to amplify the collective voice of the internet freedom community and call on those not yet engaged in internet freedom work to pay attention to the threat of internet shutdowns. To be clear, no recommendations contained in this report are meant to negate the tireless work of the internet freedom community or its achievements. Indeed, many of IRI's peers who work in this space have already mainstreamed these recommendations and best practices into their everyday operations. Still, too many CSOs, especially those that have not worked closely with digital rights organizations, have not mainstreamed these best practices. This report, particularly its recommendations and appendix, is meant to share resources and urge those organizations to adopt the best practices that have proven successful in defending CSOs and individuals from the menace of internet shutdowns.

WHAT WE KNOW

The Menace of Internet Shutdowns

Today, the promise of a free, open, and interoperable internet faces strong authoritarian headwinds. According to Freedom House's 2022 Freedom on the Net report, "global internet freedom declined for the 12th consecutive year."[2] The report finds that "the internet is more fragmented than ever, with a record number of governments" restricting access for billions of users.[3]

"The most extreme and draconian" of these censorship tactics are internet shutdowns.[4] Open Technology Fund (OTF)[5] defines an internet shutdown as a disruption, "imposed or directed by state authorities, which indiscriminately limit[s] or wholly restrict[s] access to the global Internet."[6] This includes total and partial shutdowns, as well as throttling. The most severe of these is a total (or blanket) shutdown, a complete internet blackout in which the government cuts all access.[7] Shutdowns have a wide range of technical implementations, and target different portions of the population, from neighborhoods to entire countries, and include social media blocks and mobile internet shutdowns.[8] Shutdowns manifest across a spectrum including daily curfew-style events to years-long blackouts, and can be imposed by states, police forces, and warring parties.[9]

[2] Funk, Allie, et al. "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet." Freedom House, 2022, freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet#tracking-the-global-decline

[3] Funk, et al. "Freedom on the Net 2022."

[4] Schwartz-Henderson, Laura. "Building Capacity for Internet Shutdown Advocacy: A Community Needs Assessment." Internews, 24 Nov. 2020, internews.org/blog/building-capacity-for-internet-shutdown-advocacy-a-community-needs-assessment-report/

[5] Open Technology Fund (OTF) is an independent non-profit organization focused on global internet freedom.

[6] "OTF Debrief—Introducing the Shutdown Getdown." Open Technology Fund, 16 Feb. 2023, opentech.fund/news/otf-debrief-introducing-the-shutdown-getdown/

[7] Abrougui, Afef. "Internet Shutdowns and Elections Handbook." Access Now, April 2021, accessnow.org/internet-shutdowns-and-elections-handbook/

[8] For a more nuanced, technical explanation of the different types of internet shutdowns, see Access Now's taxonomy of internet shutdowns: Björksten, Gustaf. "A Taxonomy of Internet Shutdowns: The Technologies behind Network Interference." Access Now, June 2022, accessnow.org/cms/ assets/uploads/2022/06/A-taxonomy-of-internet-shutdowns-the-technologies-behind-network-interference.pdf

[9] Rosson, Zach, et al. "Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022." Access Now, Feb. 2023, accessnow.org/cms/assets/uploads/2023/02/KeepItOn-2022-Report.pdf

Internet shutdowns continue to be a mainstay in many authoritarians' toolboxes. In fact, Access Now and the #KeepItOn coalition, the leading coalition working on internet shutdown advocacy and prevention, "documented at least 564 shutdowns around the world... between 2018 and 2020."[10] In 2022 alone, Access Now and the #KeepItOn coalition documented 187 shutdowns in 35 countries, including Bangladesh, China, Cuba, Ethiopia, India, Iran, Myanmar, and Sudan.[11]

Why Internet Shutdowns Matter

Internet shutdowns matter because they violate human rights and disrupt societies. The rights to free expression and the free flow of information are fundamental, longstanding and codified in the Universal Declaration of Human Rights.[12] In addition to violating human rights, internet shutdowns cause widespread disruptions. Internet shutdowns, especially blanket shutdowns, do not have neat borders. They affect a much broader swath of the population than just human rights activists. Ordinary people, going about their daily lives, lose access to routine, and even essential services during a shutdown. When authoritarians shut down internet access, they also shut down access to all health, educational, social, political and economic resources that live online.[13] For example, business owners cannot process online transactions during a shutdown. During a telecommunication shutdown, people cannot reach emergency services or contact their loved ones.[14] These disruptions can be especially dire considering that shutdowns often coincide with periods of unrest and human rights abuses, such as police violence or arbitrary detentions.[15]

The Internet Freedom Community

A robust and growing coalition of international organizations is leading the fight against internet shutdowns. An entire community of implementers, funders, advocacy organizations and technologists works hard to strengthen democratic resilience to internet shutdowns. The internet freedom community has "played a leading role in first identifying and raising awareness of [the] problem, often tirelessly over years, and then creating a strategy to address it, with assistance from others who can organize the requisite financial and political resources."[16] While implementers, funders and technologists collaborate to develop, distribute and maintain internet freedom tools, advocacy organizations condemn internet shutdowns and work to hold authorities responsible when they disrupt the free flow of information. Access Now and #KeepItOn coalition, for example, engage governments before, during and after shutdowns to urge authorities to #KeepItOn.

The internet freedom community has made hard-fought progress, but cannot vanquish digital authoritarianism to the ash heap of history alone. Freedom House's 2022 Freedom on the Net report recognizes these efforts have begun to move the needle. "A multipronged effort including strategic litigation, evidence-based research, multilateral and bilateral engagement, and targeted advocacy has changed the behavior of governments imposing shutdowns," the report acknowledges.[17] For example, the incidence of blanket shutdowns is decreasing, as today's shutdowns tend to be "more localized and temporary" than their predecessors.[18] Despite this progress, the problem persists, and authorities continue to shut down internet access at an alarming rate. The number of countries that shut down internet access reached an all-time high in 2022, and the total number of internet shutdowns has remained high for years.[19]

[10] Abrougui. "Internet Shutdowns and Elections Handbook."
[11] Rosson, et al. "Weapons on Control, Shields of Impunity."
[12] Article 19 of the Universal Declaration of Human Rights, un.org/en/about-us/universal-declaration-of-human-rights.
[13] Sarkar, Torsha, and Laura Schwartz-Henderson. "Internet Shutdown Advocacy in India: How to Prepare, Prevent Resist." Internews, preparepreventresist.org/india-2/. Accessed 3 May 2023.
[14] Abrougui. "Internet Shutdowns and Elections Handbook."
[15] Rosson, et al. "Weapons on Control, Shields of Impunity."
[16] Funk, et al. "Freedom on the Net 2022."
[17] Funk, et al. "Freedom on the Net 2022."
[18] Funk, et al. "Freedom on the Net 2022."
[19] Rosson, et al. "Weapons on Control, Shields of Impunity."

A Lack of Preparedness

On balance, civil society's response to internet shutdowns tends to be reactive. Too often, CSOs find themselves unprepared. Despite the achievements and global reach of the internet freedom community, statistics show that the problem persists. A 2020 global internet shutdown needs assessment by Internews' OPTIMA project found that resource constraints and a lack of technical expertise (such as accurate and localized information on internet freedom tools) leave many CSOs playing catch-up when a shutdown occurs.[20] This assessment also found that a majority of organizations, especially those that self-identify as outside of the internet freedom space, reported little to no preparedness for internet shutdowns.[21] Critically, 84 percent of respondents outside the internet freedom community (such as human rights and media organizations) reported that they had no plan for what to do in case of an internet shutdown.[22] Of these organizations, 60 percent reported that they had never used shutdown preparedness resources or tools, and 55 percent reported "that they were unaware of other organizations in their country or region who could assist them if an internet shutdown should occur."[23] Overall, the Internews report finds that strategies to assess the risk of internet shutdowns "are not conducted regularly or in a systematic way."[24]

Recent country-specific assessments in India, Bangladesh, Tanzania and Senegal echo these findings. While familiarity with individual internet freedom tools varies by country, these surveys show one common thread: a general uncertainty about how to go about preparing for internet shutdowns.[25]

The Need for a Proactive Response

Discussions within the internet freedom community often repeat the same troubling set of facts. The threat of internet shutdowns is growing. Internet shutdowns threaten the fundamental human rights of billions of people. Yet, most civil society organizations remain unprepared to mitigate the threat. When a shutdown occurs, digital rights groups, donors, and implementers receive requests for tools and resources to help local partners. Last-minute emergency responses often prove futile, however, because the same channels needed to share and download this vital content are under attack. For example, during a shutdown, local CSOs may not be able to connect to the internet or app stores to download useful internet freedom tools, nor would they have access to any how-to guides and tutorials that live on developers' websites. Clearly, a more proactive response is needed. In this report, IRI and its partners hope to advance the conversation and urge stakeholders across the DRG community to address this glaring vulnerability by building a proactive response to internet shutdowns.

> ***Last-minute emergency responses often prove futile, however, because the same channels needed to share and download this vital content are under attack.***

[20] Schwartz-Henderson. "Building Capacity for Internet Shutdown Advocacy."
[21] Schwartz-Henderson. "Building Capacity for Internet Shutdown Advocacy."
[22] Schwartz-Henderson. "Building Capacity for Internet Shutdown Advocacy."
[23] Schwartz-Henderson. "Building Capacity for Internet Shutdown Advocacy."
[24] Schwartz-Henderson. "Building Capacity for Internet Shutdown Advocacy."
[25] Sarkar and Schwartz-Henderson. "Internet Shutdown Advocacy in India."; Chowdhury, Miraj, and Laura Schwartz-Henderson. "Internet Shutdown Advocacy in Bangladesh: How to Prepare, Prevent Resist," Internews, preparepreventresist.org/bangladesh-3/. Accessed 3 May 2023; Diagne, Daouda, and Laura Schwartz-Henderson. "Internet Shutdown Advocacy in Senegal: How to Prepare, Prevent Resist," Internews, preparepreventresist.org/senegal-2/. Accessed 3 May 2023; Njogu, Wakini, et al. "Internet Shutdown Advocacy in Tanzania: How to Prepare, Prevent Resist," Internews, preparepreventresist.org/tanzania-2/. Accessed 3 May 2023.

THE INTERNET FREEDOM WORKING GROUP

Goals

IRI established the Internet Freedom Working Group to facilitate greater collaboration and coordination within and beyond the internet freedom community. Recognizing that no organization can solve the world's internet freedom challenges alone, the IFWG created a forum for experts already engaged in internet shutdown-related work to come together to share resources, tools, and best practices. Building off these discussions, IRI has synthesized the best practices shared by this dynamic community into this report, which outlines a proactive approach to internet shutdowns. This report seeks to elevate the voices of those working tirelessly to fight back against internet shutdowns, and to push others to consider the risk and plan ahead.

Composition

The IFWG included a group of core members and guest speakers. Core members included 12 to 15 practitioners from across three key stakeholder groups: funders, implementers and technologists. Organizations included in this core group were Access Now, Internews, IRI, Google Jigsaw, National Democratic Institute (NDI) and OTF. IRI determined core members based on discussions with funders and partners. By keeping the core group small, IRI ensured that discussion stayed focused on achieving the IFWG's main goals. In addition to the core members, IRI also brought in a curated set of subject-matter experts relevant to each session.

Achievements

In total, the IFWG convened six sessions that proved adaptive and collaborative. Flexibility in session topics allowed the IFWG to cover big-picture questions in some sessions, while adapting others to address timely crises, such the war in Ukraine and protests in Iran. IFWG members collaborated throughout to share resources, tools, and best practices. The appendix of this report provides a list of resources shared by IFWG members, including Access Now's Digital Security Helpline and various tools and resources recommended and created by Internews, Jigsaw, OTF and others.

METHODOLOGY

IRI prepared the following list of recommendations in consultation with the core members of the IFWG. IRI's Technology & Democracy program staff reviewed notes from each session to identify key takeaways relevant to a proactive approach to internet shutdowns and compiled a master list of recommendations grouped by stakeholder group. IRI settled on four overarching stakeholder groups: the DRG community (including implementers and actors on the ground), funders (private and government), policymakers and technologists (internet freedom tool developers).

While many recommendations overlap, IRI decided that these overall groups would best tailor recommendations to specific organization types, recognizing the distinct capabilities that each of these stakeholders has in terms of internet freedom programming. Next, program staff condensed this long list of individual recommendations into three to five specific and actionable recommendations per stakeholder. IRI circulated this condensed list of recommendations to core members for feedback via email, and dedicated the sixth and final session of the IFWG to validating and editing these recommendations. Core members helped to confirm findings, add nuance, and push back on ineffective recommendations. Based on this feedback, IRI program staff revised the preliminary list of recommendations into an improved, peer-reviewed list of recommendations. This revised list was also circulated for feedback.

RECOMMENDATIONS

For the DRG Community:

Individuals and organizations working in the democracy, rights, and governance space—including implementers and their local partners—play a key role in shifting programming from reactive to proactive. Importantly, the DRG community can help to disseminate these recommendations and associated resources to help local partners on the frontlines of internet shutdowns build their capacity to prepare for shutdowns before they occur. The DRG community can take the following steps to build a proactive response to internet shutdowns.

1. **Set up coordination channels to share resources.** DRG implementers must play a more active role in sharing internet freedom tools and resources with actors on the ground. Implementers should set up coordination channels with local CSO partners to share key resources and tools before a shutdown occurs. Implementers can do this by preparing and sharing digital "go bags" that include a set of technology that is ready to go when a shutdown occurs.

2. **Help local partners create their own Internet Shutdown Preparedness Plan**. Program teams should help partners create, implement, and practice their own Internet Shutdown Preparedness Plan.

How to Create Your Own Internet Shutdown Preparedness Plan

Assess Needs

First, implementers should help partners on the ground conduct assessments of their internet shutdown preparedness. Needs assessment methodologies, such as those developed by Internews' OPTIMA project, can help understand resource needs and capacity gaps. Based off Internews' methodology, these assessments can include: a review of internet shutdowns in the country; a survey of key stakeholders who are impacted by internet shutdowns or influential in internet shutdown advocacy; and a stakeholder focus group to validate findings, elicit feedback and identify an advocacy strategy.[26]

Prepare a Go Bag

Second, implementers should help partners create emergency action plans (the aforementioned go bags) and ensure that they are available offline in case of a blanket shutdown. To compile a go bag, implementers should work with partners to create a list of internet freedom tools and technologies to use in an emergency. This list can include digital tools (e.g., censorship circumvention and offline messaging apps) and physical equipment (e.g., foreign SIMs, satellite phones, backup USB battery packs and maps for physical meeting points), depending on the context.

Note that country context is crucial. These examples are only illustrative; they are not exhaustive, nor are they recommended in all cases. For example, in a country with robust physical surveillance, possession of a satellite phone or USB could be suspicious or even illegal, and could leave the owner at risk of search, seizure, intimidation, or detention.

[26] Assessment methodology borrowed from Internews. The Internews OPTIMA project developed a participatory methodology to work with civil societies in different countries to assess risk of shutdowns, understand the resource needs and capacity gaps, and collaboratively build responsive action plans. For more information, see: Sarkar and Schwartz-Henderson, "Internet Shutdown Advocacy in India."

In these cases, it may be best to only have a mobile device that would look innocuous and could be destroyed in an emergency. For more information on exactly what to include in a go bag, see the appendix, which compiles additional resources on internet shutdown preparedness and a list of specific tools recommended by IFWG members.

Creating a go bag is a collaborative, iterative process between implementers and local partners that requires training and testing. Implementers should help capacitate local partners by holding trainings on basic shutdown preparedness and providing a menu of tools most likely to be useful in a specific country context. Implementers should then help partners to download/acquire the tools and practice using them. By observing partners experimenting with different tools, implementers can confirm which tools work in-country and which tools users prefer. Implementers can use this feedback to hone their go bags for future use.

Practice, Practice, Practice

Third, implementers should ensure that partners regularly practice their emergency action plans. Partners on the ground should hold so-called "fire drills" annually. The training and testing outlined in the previous step provide a great first opportunity to facilitate a fire drill. Subsequent drills can be held annually with trainers or within groups or organizations. Drills allow a CSO dedicated time to practice what to do with what they have in their go bag, giving them the chance to set it up and become familiar with the technology before a shutdown occurs. Additionally, drills are a good opportunity for partners to identify and share the shortcomings of tools (so they can later be improved), and for implementers to assess what needs are not being met.

3 **Train staff on internet shutdown preparedness.** Implementers need to train their program teams on basic internet freedom preparedness so that they can, in turn, advocate for preparedness when working with partners in the field. When it comes to internet shutdown preparedness, the broader, the better. As aforementioned, shutdowns do not have neat borders; they affect a much broader swath of people than just the internet freedom community. As such, implementers' competency around internet shutdowns cannot be siloed into only small teams of technical experts.

4 **Mainstream internet shutdown preparedness beyond internet freedom programming.** Every DRG program, regardless of its focus, should consider the risk of internet shutdowns, especially those in closed and closing spaces. Any local CSO that uses social media, electronic messaging, or the internet to do its work is at risk. In an increasingly digital world, no regional program can afford to overlook the threat of internet shutdowns.

5 **Plan for internet shutdowns in advance of elections.** Implementers should recognize that internet shutdowns often occur around elections and other major political events, and should plan accordingly. To better prepare CSOs for a shutdown, implementers should include internet shutdown preparedness planning in existing pre-elections programming. Additionally, implementers should play more of a long game and consider expanding internet shutdown preparedness beyond the immediate buildup to an election. Last-minute preparation efforts are often inadequate. Planning and preparation for internet shutdowns take time, so it is best to do this important work before a CSO's bandwidth is occupied with elections activities.

For Funders:

Both private and public funders are in a unique position to incentivize actors to change their behavior by carving out explicit funding requirements for the necessary prerequisites to a proactive approach to internet shutdowns. Funders can take the following steps to encourage proactive, collaborative, and impactful programming.

1. **Require grantees to have an Internet Shutdown Preparedness Plan.** Funders should require an Internet Shutdown Preparedness Plan as part of program proposals and budgets. Specifically, funders should require recipients of funds to conduct assessments of their internet shutdown preparedness, create an Internet Shutdown Preparedness Plan, and practice the plan annually. Funders should also allow grantees to purchase equipment (such as foreign SIMs, satellite phones, backup USB battery packs, etc.) that they may need to implement their plans, as part of their budgets.

2. **Mandate quarterly risk assessments.** Funders should mandate a section covering risks and the digital environment in quarterly reports. This mandate would encourage awardees to regularly consider the threat of internet shutdowns within their country contexts.

3. **Reward information sharing.** Funding should reward organizations that share information, such as best practices, learned experiences and resources. Funders should work to build and/or maintain infrastructure that enables information sharing and collaboration between key stakeholders. Funders have a unique ability to convene actors and make forced collaboration (so-called "playdates") happen, especially before summits.

4. **Provide rapid response funding.** To the extent possible, funders should provide rapid response funds for priority needs with limited strings attached. Funders could provide some contingency funds for rapid response (as a percentage of the total award) in high-risk countries, especially where there are upcoming elections. Then, if there are any unspent funds, a funder could pool them into a rapid response fund. Additionally, funders should allow for the reallocation of funds for technology that is blocked in a country toward another similar technology (for example, from a blocked virtual private network (VPN) to a non-blocked one).

5. **Incentivize mass deployment in smaller countries.** Funders should also incentivize developers to deploy their tools in smaller countries, where they can have a greater impact. While much of the focus of internet freedom funding understandably targets large authoritarian states like China and Iran, it is important not to overlook less populous countries, such as Libya or Eritrea. In these smaller-country contexts, the mass deployment of an internet freedom tool could be adopted by a more sizable share of the population, and thus be more likely to affect broader change.

For Policymakers:

Government policymakers, in the United States and elsewhere, can help support internet freedom by clearly articulating when and where tools are legal. Policymakers can take the following actions.

1. **Build proactive programming to prepare for internet shutdowns into foreign assistance funding.** Congress can support more effective internet freedom programming by championing a proactive approach to internet shutdowns and designating funds for the purpose of shutdown preparedness.

2. **Clarify internet freedom exceptions in sanctions.** To encourage tech companies to provide services to closed places like Russia and Iran, policymakers must build more clarity and flexibility into internet freedom exceptions to sanctions. Fact sheets alone are insufficient incentives for companies worried about the risk of heavy penalties and reputational damage. Policymakers should provide a true safe harbor to companies by carving out exceptions so clearly that even a risk-averse corporate lawyer would not see a legal gray area. One way to do this is to clarify a hierarchy of sanctions, so that it is clear when an exception trumps other sanction items.

3. **Consult with technologists throughout the sanctions process.** In addition to legal clarity, policymakers must work harder to engage tool developers and tech companies throughout the sanctions process, from creation to enforcement. Policymakers should create a mechanism to allow room for advocacy, discussion, and consultation with internet freedom technologists to ensure that new sanctions do not interfere with internet freedom services, and room to discuss any suspected sanctions infractions before authorities take enforcement action.

For Technologists:

Tool developers lie at the heart of many internet freedom efforts. Through their work on back-end technical infrastructure and frontline localization, tool developers can create a more sustainable and proactive internet freedom ecosystem by following these steps.

1. **Improve the measurement of internet shutdowns.** Developers should work to improve the tools that measure and predict internet shutdowns, such as the Open Observatory of Network Interference (OONI), Internet Outage Detection and Analysis (IODA), Censored Planet, and Measurement Lab (M-lab). In particular, developers should aim to improve tools' accessibility, speed (operating in near-real time), and precision (able to measure harder-to-identify disruptions like throttling and local shutdowns). Developers should also enable tools to better predict future shutdowns and throttling, using the trends identified through past data to predict future events so early warnings can be issued. Early warning systems would allow advocacy groups to get ahead of pressuring governments not to shut down the internet.

2. **Consult with frontline users during tool development.** When developing tools, developers should work with and consult non-technical users who have firsthand experience needing to use tools to keep themselves safe. By doing so, developers can keep real-world utility, usability, and accessibility at the core of tool development. The targeting and type of this consultation matters. First, developers should take care to engage with vulnerable communities, on whom the impact of internet shutdowns is often the greatest. Second, developers should recognize, diagnose, and combat users' fears of using their tools through education, since fear of surveillance has been shown to reduce tool utilization. Through listening, targeting, and education with intended users, developers can ensure their tools are ready to be used at the frontlines of digital repression.

3. **Prioritize the localization of existing tools**. Developers can maximize their impact by prioritizing the scaling and localization of tools that they have already developed. By localizing their tools and documentation (such as tutorials) into country contexts and local languages, developers can serve more users around the world.

4. **Workshop translation and localization challenges.** Working group members noted that developers are often stuck in a perpetual cycle of translation and localization. Every app update, for example, triggers a new round of translation and localization. Developers should work together to workshop these challenges and determine what infrastructure can more efficiently and sustainably enable ongoing translation and localization needs.

5. **Prioritize open-source components**. Developers should strive to maximize their use of open-source components for their tools, especially the basic components. By doing so, developers can reuse existing code, where possible, so that new tools do not need to be built from scratch. This makes open-source code not only more democratic, but more efficient and responsive when a tool is blocked.

NEXT STEPS

In the near term, IRI will work with IFWG core members to implement the report's recommendations in their own organizations, and encourage their partner organizations, especially those outside the internet freedom space, to do the same. IRI also plans to hold public-facing events and private briefings with key U.S. government stakeholders, funders, and other internet freedom partners to disseminate these recommendations.

In the longer term, IRI hopes that the IFWG sparks action that outlives the working group itself. As members sustain the relationships they built during the year, IRI anticipates ongoing cooperation with core members to facilitate knowledge sharing and ad hoc convenings to navigate future crises.

CONCLUSION

The recommendations contained in this report are a call to action for everyone in the DRG sector—not just internet freedom activists—to take tangible steps to prepare for internet shutdowns. Whole-of-society preparedness is the only sustainable approach to a whole-of-society problem like internet shutdowns. To be clear, every human rights defender does not need to become a tech expert. Rather, the scale and frequency of internet shutdowns mean that no human rights defender can afford to ignore authoritarians' use of technology. Simple steps by actors on the ground, enabled by the key stakeholders outlined above, can be the difference between connecting when it matters most or being left in the dark. IRI recognizes that no one organization can drive change across an entire sector; collaboration will be key.

Please reach out to IRI at info@iri.org if you would like to share your inputs or collaborate with us.

APPENDIX: ADDITIONAL RESOURCES FOR CSOs

Helpline

Access Now's Digital Security Helpline offers 24/7/365, direct, secure, real-time assistance and advice to civil society actors, media organizations, journalists, and human rights defenders. The helpline offers a two-hour response time, includes circumvention tool recommendations within a holistic approach to digital safety, and operates in nine languages: English, Spanish, French, German, Portuguese, Russian, Arabic, Tagalog, and Italian.

How to Prepare Your Go Bag

- **How to Survive an Internet Shutdown**, ExpressVPN, 16 Jan. 2023.
- **Stay Prepared with a Tech Survival Kit**, ExpressVPN, 6 Feb. 2023.
- **5 Ways to Stay Online during a Government Internet Shutdown**, Rest of the World.
- **Internet Censorship/Shutdown Quick Guide:** A list of censorship circumvention tools (CCTs) to download before a shutdown occurs, available in English, Pashto, Dari, Ukrainian, and Russian.

Tools and Resources Recommended by IFWG Members

- **Bypass Censorship** is a menu of censorship circumvention tools available for download, collected by Reporters Without Borders and OTF.
- **Prepare, Prevent, Resist** toolkit by Optima is a searchable, virtual resource library featuring tools for circumvention, network measurement, advocacy, and litigation.
- Qurium's **Bifrost** is a circumvention tool that allows users to access blocked WordPress-based websites, including many in Azerbaijan, Cuba, Myanmar, Russia, and Venezuela.
- **Like Butter** is a collection of apps to make life without the internet a little smoother, and is available in English and Spanish.
- **Protect Your Democracy**, Google Jigsaw products
  - **Intra** lets you access websites and apps blocked by DNS manipulation, one of the most common forms of censorship online. It also helps protect you from phishing and malware.
  - **Project Shield** provides civil society websites with free unlimited protection against distributed denial-of-service (DDoS) attacks, a type of digital attack used to censor information by taking websites offline.
  - **Outline** makes it easy to create a VPN server, giving anyone access to the free and open internet.

Country-Specific Resources

Ukraine

- dComms provides decentralized communication during censorship and interruptions.
- "Resources to Support Users in Russia and Ukraine." Localization Lab, 11 March 2022.
- "Digital Safety Tips against Cyber Attacks in Ukraine." Access Now, 11 March 2022 (in English and Ukrainian).

Russia and Belarus

- "Digital Safety Tips for Russia and Belarus." Access Now, 15 March 2022 (in English and Russian).

Iran

- Samizdat is a browser-based tool for censorship circumvention.
- Nahoft encrypts messages to avoid surveillance.

Shutdown Measurement and Tracking

- **Access Now** reports on and condemns major shutdowns.
- **Cloudflare Radar** collects data on internet traffic, disruptions, and cyberattacks.
- **The Internet Society's Pulse** displays a map and timeline of ongoing and past shutdowns around the world.
- **OONI Explorer's Measurement Aggregation Tool (MAT)** is a database that measures connectivity to domain names, and is searchable by country and website.

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

INTERNATIONAL REPUBLICAN INSTITUTE

IRI.org
@IRIglobal

P: (202) 408-9450
E: info@iri.org