FOSStering Democracy

Threats and Successes in Counter-Authoritarian Software Development

Chris Doten, Madeleine Nicoloff, Moira Whelan
National Democratic Institute

May 2022

NDI DEM TECH NDI

FOSStering Democracy

Threats and Successes in Counter-Authoritarian Software Development

Chris Doten
Madeleine Nicoloff
Moira Whelan
National Democratic Institute

> *"First, recognize the problem. You need better conceptual framing of what you're dealing with. This is not a series of discrete tech challenges [with different] repressive applications of technology. This really is the export and spread of an entire model of digital governance and you have to recognize it as such. While authoritarians have capitalized on digitization of society as a whole, democracies have not. We have been on our back foot, we have failed to adapt to this radically new environment that has completely changed the context for democracy and the exercise of human rights and the protection of human rights. And so that's the starting place for solving these problems."*
>
> Eileen Donahoe, Executive Director of the Global Digital Policy Incubator at Stanford University, speaking at USAGM Securing Internet Freedom Event, June 30, 2021

Table of Contents

Executive Summary

The future of open societies in the digital age depends on the ability of those who believe in democracy and human rights to effectively and safely make use of the internet. To achieve this critical goal, the US government and other donors have made significant investments to develop Internet Freedom and cybersecurity tools, and global democracy implementers have had a positive impact keeping at-risk groups connected and secure. Despite these efforts, digital authoritarians appear to be winning; the rapid evolution and proliferation of aggressive tactics has made democracy and rights organizations less safe online than ever, jeopardizing the vision of an open, connected, rights-respecting democratic digital world. Democracy today can only thrive with a robust digital public sphere. In NDI's global work, this is too frequently disrupted, with partners frequently victims of hacking, internet disruptions and censorship.

Based on NDI's experiences and a range of interviews with key leaders in the Internet Freedom space, this white paper elaborates on the crisis faced in keeping democracy advocates safe online, outlines the challenges of the internet freedom technology "life cycle," and identifies lessons learned about coordination, long-term financial sustainability, and technical support to inform the democracy community. The paper concludes with a road map towards building a sustainable public interest internet freedom technology infrastructure, including recommendations for governments, donors, implementers and technologists.

Key recommendations include:

- Significant public investment in the technical infrastructure of Internet Freedom tools is indispensable for fighting back against digital authoritarians. Current efforts are successful, but should be expanded.
- An Internet Freedom Infrastructure Fund could fill a gap of long-term sustainability in support and management of proven software and resources. Even successful tools rarely achieve viability; between promising pilot and long-term success there is a "valley of death" crisis a basket fund could avoid.
- Free, open source software (FOSS) is a proven method for developing useful Internet Freedom tools, enabling wide participation in funding, designing, building, and deploying software. This process takes time as well as money, and tools cannot be wished into existence in a crisis.
- Software needs to be designed with the inclusion of marginalized groups. This requires closer collaboration between developers and democracy activists and organizers across the Global South using human-centered design approaches, and building international networks of tech-focused organizations and experts.
- Many tools can be provided as scalable cloud solutions, able to serve hundreds of thousands of users as easily and cheaply as ten; however, maladapted funding models make this approach difficult.
- Donors have a key role in forcing coordination and knowledge sharing among implementing partners and incentivizing the understanding and mitigation of security threats to partners.
- Effective internet freedom tools are not reaching the people who need them. Due to technical complexity and misaligned incentives, international development implementers rarely understand digital threats to partners or incorporate the software and approaches that could help keep them safe and connected. Donors and implementing organizations can do more to proactively integrate Internet Freedom approaches and resources into programs, and to share and apply local insights into threats on the ground.

The "digital iron curtain" that has dropped following Russia's catastrophic invasion of Ukraine on the one hand and the Summit for Democracy on the other provides two opposing visions for the future of the internet. This is a critical moment of opportunity; despite the aggression of digital authoritarians the founding vision of an open internet is still viable. Democratic activists, foundations, technologists, large

companies, governments, international development organizations, and grassroots civic groups from around the world all have a role in supporting an open internet. Internet freedom tools will be critical for activists and democratic institutions to address some of the most complex policy problems we face today, such as climate change, disinformation, violence against women, citizen monitoring, and structural injustice for marginalized communities. Larger sustained investments are required to bring internet freedom tools to scale to face the threats of today's networked dictatorships, but revitalizing democracy requires these efforts to center the internet and make it safe for all.

Acknowledgements

NDI would like to acknowledge the contributions of several individuals and organizations that have been instrumental in the development of this paper, and while we cannot name them all, we do want to thank some who were particularly instrumental in this project. While they provided a great deal of ideas and inspiration, this paper is the work of the authors and may not represent the perspectives of any of those who engaged with us. NDI would like to specifically thank Jon Camfield, Nathan Frietas, Chad Hurley, Nat Kretchun, Raphael Mimoun, and Rainey Reitman for their thoughtful interviews which were central to the writing of this paper – as well as their careers supporting at-risk democracy and rights actors.

We would also like to thank the technology teams at the International Republican Institute and the National Endowment for Democracy and particularly our colleagues at the Open Technology Fund. Collaborating on the wider project of which this paper is a small piece has been a remarkable opportunity to better understand the rich community of dedicated software developers and designers struggling to keep at-risk individuals safe and online.

This project is made possible by the generous support of the American people through the National Endowment for Democracy (NED). The opinions expressed herein are those of the authors and do not necessarily reflect the views of NED.

Definition of Terms

Terms in the internet freedom space can be confusing or even alienating for non-experts and therefore we have defined some below.

- **Cybersecurity:** Also referred to as digital security or digital safety, the art and science of attempting to keep individuals and organizations safe – in this context, particularly global grassroots partner organizations and recipients of international development funds.
- **Democracy Actors/Partners:** Democracy, human rights, legislative, or political organizations who are beneficiaries of technical assistance or funding from implementing organizations or directly from donors.
- **Digital authoritarian:** A leader, regime, or actor who uses digital information technology to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties. Tactics include, for example, the surveillance, censorship, or manipulation of information online.[1,2,3]
- **Free, open source software (FOSS):** tools built and licensed such that their source code - the instructions for the software - are legally required to be made public for others to use, modify, and share without cost. Such an approach is important with public interest technology, particularly that which is taxpayer funded, to ensure accessibility and adaptability.
- **Implementing organization:** An international NGO or contractor, such as NDI or IRI, who accepts international development funding to implement programs globally.

- **Internet Freedom:** An "open, interoperable, secure, and reliable Internet," as defined by the State Department's Bureau of Democracy, Human Rights and Labor, where individuals and organizations in our digital era are able to fulfill their basic human rights.
- **Public-Interest Technology (related to digital public goods and civic technology):** Software and technical expertise built in service of the common good. These are often tools that are built by or for public institutions such as governments or non-profit organizations.
- **The Global South:** A term for countries sometimes referred to as the "larger world" or "developing world" in which implementing organizations such as NDI and IRI work with partners and donors such as USAID, DRL, and NED provide financial support.

Introduction

The internet is an indispensable vehicle for those working to support democracy and drive positive political change around the world. Secure access to communication, documentation of human rights abuses, monitoring of censorship, and effective digital organizing have empowered activists fighting for more open societies. Technology has improved the capabilities of organizations working for social change – but at the same time has created new threats of privacy violations, online harassment, and misinformation that have shaken society and created new dangerous cleavages in democracies. Additionally, since the initial promise of digital connectivity leading directly to democratic revival that accompanied the Arab Spring, authoritarians have struck back. The organizers and activists fighting for more open, just societies with whom NDI works today are surveilled, censored, hacked, and harassed by governments and other malign actors, and neither the private sector nor existing free, open-source software (FOSS) have provided adequate tools and mechanisms to protect them.

The US government and other donors have made significant investments to develop Internet Freedom and cybersecurity tools, and organizations including Access Now, Internews, Article 19, and others have had a significant and positive impact keeping at-risk groups connected and secure. Despite these efforts, the rapid evolution and proliferation of aggressive tactics from digital authoritarians have made democracy and rights organizations less safe than ever online. Put bluntly, authoritarians are winning the digital arms race. We recognize that one key reason is that significant gaps remain in creating, maintaining, distributing, and adopting cybersecurity and Internet Freedom tools. While organizations fighting for more open societies face a host of challenges online – malign authoritarian influence, disinformation, hate speech and harassment – this paper is specifically focused on the creation, promotion, and sustainability of digital tools for at-risk actors in the Global South to keep them connected and secure. Other aspects of Internet Freedom such as improving international cybersecurity standards at a multilateral level are critical, but have been addressed in other works and are beyond the scope of this paper.

This white paper explores the reasons behind this gap and identifies lessons learned about coordination, long-term financial sustainability, and technical support to inform the democracy community. The paper captures NDI's background working with at-risk democracy and rights advocates online, experiences collaborating on a range of projects supported by the Open Technology Fund over the last year, and insights from interviews with a mix of software developers, program implementers, and funders who are active in the Internet Freedom community. In this paper we depict the backdrop of rising danger for democracy actors, document challenges to the long-term success of Internet Freedom tools, and envision a sustainable support infrastructure to empower democratic actors going forward.

The goal of this white paper is to inform policymakers funding and supporting Internet Freedom on the successes and challenges in this space to better achieve the goal of putting software in the hands of at-risk democratic actors in closing political environments. Background on democracy advocacy, human rights norms, technical aspects of connectivity, cybersecurity threats, funding for public interest technology, and more are important in discussions of Internet Freedom; this space is made more challenging by the fact

that virtually no one is fluent in all of these topics. We welcome additional perspectives and further conversation and hope this research assists in that critical effort.

The Current Democracy and Rights Tech Environment

The majority of the world is online[4,5] – and therefore the internet is required in the work of democracy and human rights. Everyone has a right to freedom of expression – as stated in Article 19 of the International Covenant on Civil and Political Rights – "this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." Internet freedom and cybersecurity guarantee the meaningful expression of this right to access a range of content through an open, secure, interconnected network, and is a necessary precondition for the exercise of these fundamental rights in the internet age.

Authoritarians and criminals are increasingly digitally savvy. Leaders of closed regimes recognize the threats that open communications and organizing pose to their control, and use internet disruptions, targeted hacking, spyware, throttling, and censorship to interfere with rights activists and everyday citizens, both within their borders and increasingly to attack democratic actors across the world. Russia's unjustified invasion of Ukraine has demonstrated the ways in which they are able to control the information space keeping Russian citizens unaware of the progress of the war, and the Biden administration has recently warned of the risks of retaliatory cyberwarfare orchestrated from Moscow. AccessNow's #KeepItOn project documenting internet shutdowns documented at least 155 in 2020 alone, many of which were related to elections or key political moments. Freedom House's Freedom on the Net 2021 report that 41% of all internet users live in countries where "authorities disconnected internet or mobile networks, often for political reasons." Since the start of the COVID-19 pandemic, there has been a significant spike in cyber attacks. As demonstrated by Pegasus hacks of human rights advocates, the global increase in ransomware, SolarWinds attacks aimed at NGOs, and a host of other threats pulled from the headlines, there is an ongoing erosion in digital safety for those who need it most and who can least afford costly protection. Authoritarian regimes are investing vast resources into development of offensive cyber capabilities – a financial commitment not matched by defensive efforts from democracies.

Escalating risks to democracy activists represent an unaddressed market failure. Democratic actors need technology tools to conduct their work, and when deployed to empower people – especially in closed environments – technology provides moments of hope and optimism that inspire movements around the world. The #BeLikeWater movements in Hong Kong, protests in Belarus, Sudan's youth-led revolution, and even individual high-profile cases of activists like Maria Ressa or Alexei Navalny have been supported by cybersecurity tools and censorship workarounds. However, the overall environment is grim; users of technology are constantly exposed to threats due in part to the low prioritization of user security by corporate actors; targeted threats against rights and democracy actors are infinitely more dangerous. While commercial platforms and cybersecurity firms provide powerful software or paid support, they do not fill all the needs for censorship circumvention and digital safety tools, often do not work outside of major languages and markets in the US or Europe, and are frequently prohibitively expensive. Commercial incentives for the for-profit sector, such as monetizing user data, or ignoring marginalized populations, can be misaligned with the goals of democracy and rights actors.

Internet freedom tools are being created, but more funding is needed for democracy actors. Groups such as the Open Technology Fund (OTF) and the State Department Bureau of Democracy, Human Rights, and Labor (DRL) Internet Freedom team provide critical but limited resources to bridge the gap between market incentives and demand for tools to defend against digital authoritarians. Civic technologists such from the Code for All Network can develop tools for local contexts, but they often lack access to sustainable funding and have limited ability to distribute their tools widely. There are more ideas generated by at-risk groups and problems identified by technology experts than financing can support today; funding systems work but are inadequate to the current crisis. While all of these investments are critical, they tend to be focused on the specific needs of human rights advocates. Democracy activists and political organizers are a specific

group with distinct needs, but they are rarely the target users for internet freedom investments, and as such their particular use cases are not typically part of software design.

Internet Freedom software cannot be wished into existence during a crisis. Even an experienced coder must navigate a complex environment for product development that, from idea to proposal to deployment, can take years. Most software developers in the larger world are unfamiliar with US government funding, and even the lightest-weight application processes such as with OTF can be prohibitively complex. At the same time, last-minute "Let's build an app!" approaches are not a responsible rapid response to authoritarian actions abruptly strangling an open internet or attacking human rights defenders; solutions need to be put in place well in advance. Professional software development approaches focused on engagement with users on the front lines supported by glacial funding cycles mean tools must be in development long before the acute localized threats are identified, and then as with any software tools and resources, must receive ongoing long-term support and upkeep. These challenges make it very difficult for new developers to join the community and contribute to the right tools in time to position for a crisis.

Funding free, open source software (FOSS) has a proven track record. Signal, Tor, CertBot, and other projects are major open source cybersecurity software achievements which have made the internet safer for all, particularly those most at risk. Free, effective, usable tools have given everyday users effective ways to communicate securely and preserve their anonymity, including in closed regimes. FOSS technology undergirds most of the foundations of the internet as a whole, from web and email servers to name services. To counter the massive investments made by closed societies in technology tools, democracies should significantly increase Internet Freedom support – with the inherent multiplier effect that open source software allows the community of open societies to publicly coordinate and collaborate on tools. Non-market-driven donor funding sources, such as foundations and the US government, can and should prioritize the needs of Global South groups often neglected in commercial software development, including marginalized communities such as women, persons with disabilities, those with low levels of education, those with limited bandwidth or costly internet access, and non-English speakers.

Successful tools are rarely able to achieve long-term viability. When prototype tools are regularly developed successfully with startup funding, few projects are sustained over time. This squanders the initial investment, leads to reinvention of wheels, and detracts funding from other essential tools. Even during the course of this research project, several significant and popular tools such as FrontlineSMS made the difficult decision to close their businesses. In their explanation, they cited the difficulty of achieving long-term viability as the primary driver for their demise.

The appropriate resources are not reaching democracy and rights actors. Thanks to investments in this space, there are useful FOSS cybersecurity and Internet freedom tools available to fill market gaps for democracy and rights actors. However, these at-risk groups are often unaware of the threats they face – and the availability of internet freedom tools that could help protect them. Implementing organizations typically share the same blindness to cybersecurity threats and are often not incentivized to provide internet freedom tools, despite their general responsibility to mitigate harms to partners. Even with the right solutions in hand, it can be challenging for any of us to use new software. Cybersecurity and internet freedom problems are complex, and tools to solve them are as well. These challenges are exacerbated by the fact that developers in this space rarely have the skills for building user-friendly products, and there is little in the way of training and support to help when people get stuck.

Talented democracy and rights-focused software developers are leaving the field. Due to the start-and-stop nature of grant-based international development funding, it is challenging to build successful businesses and careers. One developer of a successful product described how he was unable to provide benefits for his staff because of intermittent funding. Salaries are entirely uncompetitive with the private sector; developers do not expect to be paid as at a major technology company, but it should be commensurate with their talents. As it is, developers leave when they have family obligations, or join after making big money in the

private sector, but few can make a viable career in rights-focused public interest technology. This churn makes for a constant loss of knowledge, mentorship, and trusted personal relationships.

Democracies face a critical moment of opportunity. While the challenges are daunting, there is a chance to imagine a new framework for supporting democracy and human rights despite the aggressive attacks of digital authoritarians, empowering those using the internet to build more open societies. The new US administration provides an opportunity for learning from the past and a departure from flawed models. After the challenges of the last years, the Open Technology Fund has reestablished itself as a core pillar in this critical space, along with other mainstays such as the State Department DRL Internet Freedom team. USAID, the largest funder of international development, is increasing investments in this space through large vehicles such as the current Greater Internet Freedom program, and a wide variety of individual projects. The new USAID Digital Strategy provides a roadmap for implementers and beneficiary partners to systematically include cybersecurity and internet considerations in development work. Expansion of existing Internet Freedom funding efforts, increased coordination, and new models for sustainable support can take advantage of this moment to face the rising authoritarian threat and reinforce the system for building software that supports democracy in the digital age.

The Counter-Authoritarian Software Lifecycle

The U.S. government and other donors have built an ecosystem to create Internet Freedom and cybersecurity software for those working for democracy and human rights in closing spaces over the past decade. Many components of the ecosystem are successful, others need improvement, and some do not function well. In this section we provide a highly simplified overview of the tool-creation process from idea to arriving in the hands of at-risk actors, identifying successes, challenges, and recommendations for each step of the process.

Phase	Successes	Challenges	Recommendations
Identify solutions to authoritarian threats	Donor and developer leadership are focused on well-documented internet freedom problems, and dedicate attention and resources to addressing them.	Grassroots organizations rarely have technical visibility into the attacks or censorship they may encounter. Implementing organizations and less technical donors do not know what threats their partners face, and therefore do not build countermeasures into their program plans or share emerging threats with donors. There is a disconnect between internet freedom technology developers, often in the US or Europe, and priority needs at the local level. Few of the non-technical local partners and implementing organizations closest to threats provide input informing decisions in the tool funding space.	Implement distributed data collection on cybersecurity attacks and digital censorship with a range of democracy advocates to see trends in threats to Internet Freedom. Increase coordination between academic institutions, major tech firms, and local technical expertise to understand and analyze threat data collected from non-technical groups. Establish better channels of communication between grassroots democracy partners, implementing organizations, and the Internet Freedom community to provide timely awareness of evolving threats for Internet Freedom developers Prioritize knowledge sharing and solution distribution across silos and implementing organizations on the problems faced and

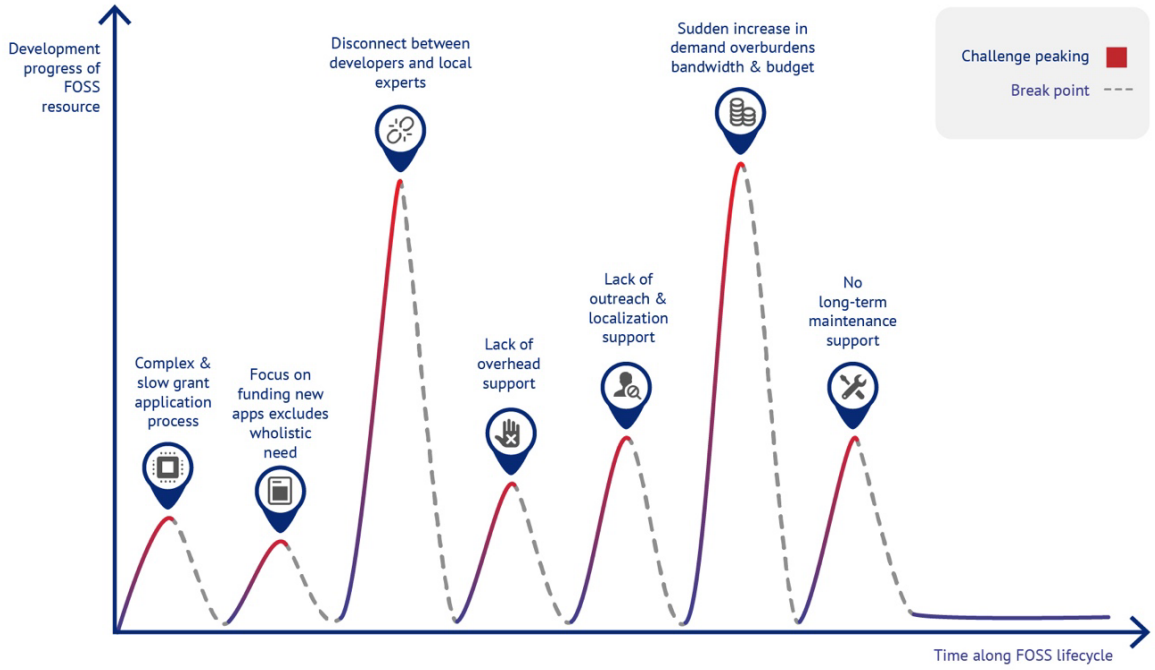
			approaches taken by partners.
Fund the most critical internet freedom software	There is generally effective coordination among Internet Freedom-focused donors, with frequent informal conversations among OTF, DRL, and other groups reducing duplication of efforts from the funding perspective. OTF provides good opportunities for developers from the Global South to submit responses to the challenges they see through their open calls. OTF and DRL provide critical funding that has successfully launched many useful FOSS projects.	Given the compartmentalized regional nature of international development work, patterns of problems or promising ideas are often siloed, leading to reinvented wheels or repeated mistakes. Internet freedom problems faced by partners are often funded in an ad-hoc and non-strategic way by less technical organizations. The funding ecosystem is complex and hard to navigate for technology developers, with complex applications, lengthy timelines, and limited process visibility. Government procurement processes are challenging and cumbersome to those not already used to working with donors, particularly from the Global South. This is particularly true for working with technology vendors. Pilots need to fit into a narrow category to be eligible for internet freedom funding. Software that could, for example, protect the data of at-risk rights and democracy groups may not make the cut. The long timeline of Internet Freedom funding often means that technology is overtaken by events either from a technology or a user need perspective. The community is far less nimble than authoritarian adversaries.	Develop clearer USG application processes, timelines, and status updates translated into multiple languages. Find ways to reduce time from application to program start to a few months. Establish funding that incorporates an agile approach to project management and implementation where all aspects of solutions cannot be known in advance. Donors should recognize that funding in this space will entail justifiable risks. Establish smaller microgrant funds targeting developers from the Global South with limited application and reporting requirements, ideally managed by local technology organizations. Develop broader definitions of projects that support internet freedom objectives, to include public interest technology more generally.
Build a sustainable internet freedom developer community	Talented, committed individuals work successfully in this space to build world-class software products.	Salaries and benefits for Internet Freedom developers do not come close to matching the private sector, leading to ongoing turnover and limited recruitment. There has been limited success identifying developers from the larger world and cultivating them for participation in the Internet Freedom software development community.	Align developer salaries and benefits to be broadly competitive with the private sector. Foster and fund a network of local technologists in multiple locations in the larger world, providing a pipeline of talented developers, trainers, testers, designers, and consultants integrated in the local context. Provide long-term core funding for proven Internet

			Freedom software development organizations to provide stability for developers.
Develop and deploy successful Internet Freedom tools	Donors such as OTF and DRL ensure new tools make it into the hands of a limited group of at-risk target users. The Red Team Lab, sponsored by OTF, does an excellent job of providing security auditing support to Internet Freedom tools.	Software is not always built in a human-centered fashion, particularly with regard to marginalized communities. There is no structural accountability ensuring implementing program officers focus on critical internet freedom issues and integrate them in international development programs appropriately.	Establish an institutionalized process of oversight to integrate relevant Internet Freedom and digital security priorities across all international development sector silos. Set expectations of all implementing desk officers that they have a basic understanding of the challenges and opportunities to keep partners safe and connected, and that they share the problems their partners encounter with technical teams. Expand engagement with OTF's Usability Lab (similar to the Red Team Lab) to provide user-centered design support to more tools. Consider additional lab-style support mechanisms for scalable provision of useful skills for developers such as dealing with donors or marketing.
Scale high-impact counter-authoritarian software	FOSS Internet Freedom products are cost-free to partners and relatively accessible. Viral spread and uptake – particularly in moments of political crisis – can be highly successful. Successful open source components that provide an individual element of functionality are sometimes integrated across a range of tools, such as the Signal protocol into WhatsApp. There is an excellent community of translators with experience in Internet Freedom space, particularly Localization Lab.	There is not typically funding for any form of advertising or outreach about new products, limiting spread Partners are unaware of the threats they face, and the tools they could use that would mitigate those threats. Even with knowledge of threats, partners may be reluctant to implement new technical systems. Tools and related documentation are often not localized and translated into languages that would be useful. Implementing organization staff in the democracy community but also in the broader international development community (health, education, etc) are not aware of the range of tools that are available or the	Focus on technical capacity building of local democracy and human rights partners' digital security and Internet Freedom awareness so they understand basic threats and opportunities. Establish funding and donor coordination focused on scaling the implementation of tools that have completed the pilot phase and demonstrated capability to successfully meet users' needs in order to reach new democracy partner user bases. Non-technical donors and implementers should inform themselves of internet-freedom related tools and approaches to mitigate threats, and mandate their inclusion in calls for proposal or proposals.

		problems they solve and do not include them in proposals. Partners who hear about and are interested in tools do not always have the skills to install and run them. Documentation and training to fill those gaps are lacking.	Distribute a "catalogue" of the Internet Freedom tools and resources available and the range of problems they can solve, making it easier for partners and program designers to build them in. For an example, see the list of NED-family supported Internet Freedom projects incubated by the OTF. Permit marketing and advertising costs as a part of software development agreements. Internet freedom-focused donors and implementers need to better connect outside of their small community to share tools and approaches. Foster a global community of tech-focused NGOs familiar with these tools able to provide trusted local capacity building, tool-specific training, and long-term support. Encourage developers to develop individual technical Internet Freedom components that can be used on a modular basis across multiple tools. The collaborative nature of the community means organizations need not develop entire software suites.
Respond to digital authoritarian crises	For existing tools, the FOSS community is a good foundation for the rapid scaling of a product. Democracy programming is flexible for urgent unforeseen contexts.	The sudden increase in demand during a crisis can burden a tech company – success can mean huge costs in bandwidth, demands for support or translation, etc. When a crisis occurs it is too late for the iterative software development and user testing that makes tools as effective as possible. Authoritarian actors are outlawing specific tools used by democracy actors such as VPNs and using in-country corporate staff as hostages.	Establish contingency funding for surges in demand such as bandwidth and hosting costs, additional technical support, or needed translations. Ensure that implementers and democracy actors work in advance of crises to build resilience towards common threats of shutdown or attack by distributing tools and localizing resources. Democratic governments provide political support to companies facing authoritarian pressure.
Maintain internet freedom software over time	Hosted online software scales – internet-based platforms	Even the best pilots rarely make it to long-term viability and scale. There are few replicable paths to	Provide core infrastructure funding for proven tools at a predictable level for a long enough time to provide

	can serve millions with very small incremental costs. Building upon past investments in software development through human-centered research on products in use, particularly in marginalized communities, can generate ongoing improvements that lead to greater uptake	sustainability of Internet Freedom tools, leading to wasted or repeated efforts. Software or training resources require ongoing support to stay up to date in the face of constantly evolving threats, but ongoing support for incremental improvements is difficult to fund. This leads to the tools or resources becoming out of date. Donors prefer to fund new projects or components rather than providing the supportive funding required to keep things going. At times, this leads to building new features simply to provide the funding for maintenance. There is not a vibrant FOSS developer community around most products. Most contributors are affluent white males who lack understanding of the needs of the larger world. Commercialization, sometimes seen as the long-term sustainability path for a given Internet Freedom product, is rarely profitable. If so, a new problem becomes the public mission subsumed by chasing market success. Scalable hosted software requires ongoing funding for support which does not mesh well with the standard donor grant program model.	stability for organizations. Develop a process for accepting new projects with the most potential, and winding down funding for those who are not achieving targets. Build requirements for iteration and improvement into long-term funding, particularly for human-centered design with marginalized communities. Invest in additional language localizations based on demonstrated demand. Build a global coalition of internet freedom software developers working across multiple FOSS with supportive community management and incentives. Break down some of the culture of isolation and secrecy in the Internet Freedom space. Tools that are a secret are hard to distribute or build a community around. Encourage major technology firms to mainstream appropriate components of Internet Freedom tools into their work, and provide sponsorship in the form of free hosting credits, technical assistance, or contributions to Internet Freedom infrastructure fund baskets.
Retire obsolete internet freedom software	Donors such as OTF and DRL are aware of the risks of unsupported software and encourage developers to retire projects appropriately. When many projects shut down, they attempt to do so in an orderly, responsible way, such as FrontlineSMS.	Non-technical donors and programs tend to develop software and then move on; retirement and decommissioning is not part of routine program design. Software that is no longer supported is at elevated risk for vulnerabilities; this is particularly true with security software.	Ensure that non-technical donors understand that products do not live forever, and that they have appropriate decommissioning processes in place for security reasons. Ensure there are channels in place to inform users of when tools have been retired and that they should stop using them. Make retrospective reviews a part of the decommissioning/shutdown

			processes to share lessons learned.



Recommendations for Building a Lasting Counter-Authoritarian, Pro-Democracy Internet Ecosystem

In recent years the democracy community has broadly come to accept that the futures of the internet and of open societies are inextricably linked. Funders have recognized the importance of building sustained global investment to address critical challenges posed by malign authoritarian actors, and have provided early support to establishing today's vibrant Internet Freedom technologies to help protect democratic movements. While developing these tools is not the complete solution to countering digital authoritarians, it is a necessary technical foundation undergirding a multilayered approach to protect democracy and rights actors at greatest risk.

Committed developers and knowledgeable funders in the Internet Freedom community have done admirable work filling the market gap for essential tools to keep human rights activists and democratic organizers safe and connected online. However, these tools have little chance of becoming long-term successes without a sustainability model that permits most to make it through "the valley of death" – the grim term used by more than one developer for the failure that looms between most successful pilot projects and long term success. Sustainability in the current system is a mirage, and as a result, the democracy community is significantly limiting its ability to compete against authoritarians in the struggle for an internet that empowers rather than suppresses democracy and human rights. Further, implementing organizations do not do enough to ensure the successful use of these tools by at-risk organizations or to elevate the threats they experience to developers. The pieces are in place to

identify problems and build tools that make a difference in the hands of partners, but creative thinking and new funding models are required to take advantage of these opportunities and end the cycle of squandering time and resources on short term solutions in the Internet Freedom space.

Drawing upon the UN Declaration Human Rights and as a matter of US policy, the clear objective of Internet Freedom is an open, interoperable, reliable, and secure internet. A broad-based, resilient, open, and well-supported community is required to make that vision of a safe, connected world happen, with leadership from governments, creative funding from donors, talent from technologists, support from implementers, and flexibility from democratic actors. We have identified several critical next steps for the core participants in the counter-authoritarian software ecosystem below.

Key Recommendation: Create a new "Internet Freedom Infrastructure Fund."

Long-term success against digital authoritarians requires a new approach for long-term funding of Internet Freedom software. To address critical sustainability challenges a dedicated, coordinated fund should be created to maintain successful open source internet freedom tools which have proven their capabilities to support an open, secure, counter-authoritarian internet. Like other forms of public infrastructure, public interest technology requires ongoing support and investment which such a fund could provide. Supporting sustainability is cheap compared to the wasted effort and ongoing reinvention of wheels required with new projects. Moreover, investing in scale – providing the ability for these internet freedom tools to reach millions of people – is a particular bargain, supporting far more people for a tiny fraction of the cost of one-off solutions.

A specialized team is required to manage Internet Freedom funding. The dedicated funding supporting such an Internet Freedom Infrastructure Fund could be maintained through an organization such as OTF, an expanded State Department DRL team, or a donor organization in direct contact with a wide range of democracy partners such as the NED. However, given the specialized nature of this work, it may be appropriate to create a new organization with a unique, focused and singular mandate of development, investment and infrastructure in the digital world: instituting norms and standards, providing direct long-term support for proven projects, and promoting sustainable business models for innovations. Wherever housed, such a fund would require staffing by an array of specialists, including technologists, policymakers, and democracy professionals.

A basket fund permits an array of donors to benefit from the same tech expertise. Coordination on these issues is challenging. A basket fund led by the US but welcoming contributions by other governments, foundations, and corporations would enable many to support these efforts without needing to duplicate sophisticated technology assessment on deserving products. Operating transparently to donors and partners alike, an Internet Freedom Infrastructure Fund would have a mandate to connect with the talents provided by OTF, DRL, and other technical communities, as well as to provide more direct, deep engagement with the wider international development, democracy, and human rights community. The use of free, open source software provides a collaborative space in which a range of global donors, developers, and implementers can support at-risk democracy organizers and human rights advocates together.

Current Democracy and Rights Tech Environment

Healthy Democracy and Rights Tech Environment

Governments Should:

Connect the world so all can participate online. While a majority of the world is now connected to the internet, that still means almost half are not. Those in this enormous gap are politically marginalized, unable to take part in the digital public square or access critical resources. People without access are disproportionately at the fringes of society to begin with, such as in rural areas or impoverished communities. Major investments in physical infrastructure are critical to reach those left behind and ensure that access is affordable for all. When designing this infrastructure, the norm should be that open, democratic governments build resilient networks, with a wide range of connections and across different technologies to make disruptions – accidental or intentional – more difficult. Network equipment should not be hardwired for surveillance and censorship, which is often the case for hardware purchased from China.

Ensure a supportive regulatory environment for internet freedom. Ultimately, the legal regimes under which users, developers, and network operators will enable or undermine Internet Freedom. The implications of the internet are complex; thoughtful regulation requires that legislators and their staff gain a basic level of technical understanding. Encouraging engagement with civil society can help bridge some of these knowledge gaps, and as such multi-stakeholder inclusion is valuable in crafting domestic and international regulation. Lawmakers should create structures that protect data privacy, limiting surveillance by the state or corporate actors, and do not restrict encryption or systems for maintaining anonymity.

Create incentives for tech corporations to prioritize security. As demonstrated daily through incessant hacks on users and their personal information, vulnerabilities in software created by for-profit companies have vast costs. While this is usually measured in dollars of economic loss, there is a far higher price paid by at-risk organizers and activists; software bugs become dangerous vulnerabilities which are exploited through targeted hacks such as in software from the NSO group, or mass attacks targeting NGOs. Governments can incentive structures through which corporations must bear some liability for the damage by digital authoritarians caused by flaws in their products.

Emulate successful vaccine supply chain models for tech. An example of a positive collective effort is Gavi, the Vaccine Alliance. Gavi's core goals include creating a reliable and affordable supply of vaccines; scaling transformational innovations to increase equitable access; working with communities to increase trust and build resilient demand; and strengthening delivery systems. These same strategic approaches are needed to address the challenges faced in the struggle for a free and open internet: creating reliable tools that can be trusted in the long term; scaling innovations to reach new audiences; helping at-risk communities understand their threats and building tools that address them; and building technical capacity, data analysis, and effective access to tools for those who need them. This model, with a range of donors feeding into the same pool, should be replicated for the Internet Freedom community.

Demonstrate a public commitment to democracy technology. The bold step of starting the Open Technology Fund (OTF) sent a strong message that the US is dedicated to an open internet and access to fact-based journalism. A similar commitment to the democracy community is an appropriate response to today's rising authoritarian threat. Donors including OTF and State Department Bureau of Democracy, Human Rights, and Labor (DRL) Internet Freedom team have a proven track record of helping new Internet Freedom and digital security tools go from identified partner problems to products in the field, but are focused on human rights actors more than the needs of the democracy and governance community. Expertise from an organization such as the National Endowment for Democracy (NED) could similarly bring critical subject matter expertise and connections with partners. Continuing to choose inaction in the democracy and governance space cedes the digital arena to authoritarian actors with the stated objective of manipulating and limiting political participation.

Funders Should:

Expand funding for the Internet Freedom software layer to keep people connected and safe. While the internet has physically connected much of the world, achieving the original vision of a network which

reinforces open societies requires a much wider Internet Freedom software infrastructure layer to fight censorship, surveillance, and targeted attacks. Without the ability for pro-democracy actors to use the internet safely and effectively, this network built at enormous cost by the US and other open societies is devolving into a playground for digital authoritarians. More financial support, ongoing experimentation, and rapid evolution is required to face the well-funded authoritarian threat which will inevitably create risk; learning through failure will be a necessary part of this process.

Break down organizational silos to share counter-authoritarian experience. Donor organizations should continue to focus on their specialties, but with a better integrated approach that acknowledges the capabilities and contributions of other groups. As one interviewee commented, due to internal bureaucratic incentives inter-organizational rivalries and silos are real, and interfere with delivering effective results for partners on the ground. Common challenges to deployment of Internet Freedom tools can be addressed quickly, such as clarifying funding cycles, providing standardized training on grant writing, coordinating problem identification and funding, managing donor support handoffs from pilots to sustainable products, and filling other bureaucratic gaps. Less technical donor organizations or internal departments should increase their knowledge of Internet Freedom and build closer connections to benefit from the expertise of more technical donor organizations. At the same time, the secrecy and jargon of Internet Freedom technology can make the space forbidding for those less technical donor groups, and the technical community has an obligation to engage more frequently and in ways others can understand. One interviewee described the internet freedom community as a "Galapagos Islands" of interesting ideas disconnected from the rest of the world – which also isolate their impact.

Enforce the responsibility to protect partners regardless of sector. Internet Freedom and cybersecurity threats exist in all developmental sectors, but apart from those explicitly focused on authoritarian threats there is not currently adequate investment to protect partners given the looming threats. Even across democracy and governance programs there is currently no mandate for universal emphasis on integration of responsible cybersecurity and Internet Freedom software which can empower and protect all sectors of development. Donors have the power to incentivize this emphasis on Internet Freedom by mandating responsible protection of partners in calls for proposals and reporting requirements.

Support the true costs of a professional technology workforce. Free, open source software is not free to build, and donor agencies need to support the true costs and salaries of organizations and employees building these tools. The democracy community relies on professional software developers, but many organizations are unable to offer benefits or employment security to their staff due to the vagaries of their funding. Few come close to matching private-sector salaries, and therefore often rely upon people who soon feel obligated to join the for-profit sector, or to the occasional engineer who has made so much money that they no longer mind an inadequate salary out of a desire to give back. This excludes a wide range of talented individuals from around the world, particularly those from diverse backgrounds and marginalized groups. As one interviewee commented, "hoping for unicorn software developers is not a strategy." Similarly, costs of office space, computers or software, travel to conferences to meet users and share tools, funding for marketing of products, ongoing training, and other activities that are not directly focused on creating products are key needs for healthy organizations but are not funded by donors, hamstringing this work.

Provide rapid response funding for useful tools in crisis situations. At times of highest need – for example, in the case of a VPN providing uncensored access in a country where political turmoil has led to an internet blackout – the fact that software is successfully solving a problem can create new problems: huge increases in users can create costs in additional bandwidth, demands for new translations, needs for technical support, risks of targeted hacks, or other challenges that can overwhelm or even break a tool. Currently no structure exists to provide rapid support in this scenario beyond a patchwork of volunteers and ad hoc emergency funding to keep critical cybersecurity tools operational. Moving useful tools to funded platforms built for rapid scalability will also add resilience in these critical inflection points for democracy.

Fund the long-term sustainability of proven products. Technology projects which have demonstrated initial success often find themselves in a particularly challenging position. Having been funded through the pilot stage, they have demonstrated that their tools provide genuine value for an interested audience. Organizations that have been able to access relatively smaller initial funding through, for example, OTF, now find the need to keep their project running, though without the potential markets to attract venture capital support, knowledge or time for managing complex donor relationships, or a client base for a commercial offering. The organizations who do manage to endure in this space do so through a cobbled-together collection of grants and projects, none of which provide long-term stability or predictability. This is a key gap that could be addressed by the Internet Freedom Infrastructure Fund described above: a dedicated stream of funding for the long-term maintenance and support of essential tools.

Fund scalable systems to reach global audiences. Popular FOSS tools like Eclips.is secure hosting and Deflect denial of service attack protection serve large communities, but it is difficult to distribute that cost to thousands of beneficiaries across scores of programs, and there is no model for funding them through current mechanisms. The power of modern cloud-based hosting can scale tools to vast numbers of users with very low marginal costs, making it a far more efficient use of donor funds. Having large numbers of users on shared, scalable hosting space is not only cost effective, it provides access to greater insights. By seeing how groups of people, particularly those from marginalized communities and across different regions, engage with tools developers are able to better understand what is working and what is not. Common infrastructure provides better minimum security standards, and attacks on such shared infrastructure can be monitored by more sophisticated cybersecurity analysts to reinforce those tools and build resilience in the community as a whole. The proposed Internet Freedom Infrastructure Fund could be well positioned to pay these marginally low but ongoing costs.

Global NGOs and Implementers Should:

Prioritize their responsibility to keep their partners safe. Given omnipresent authoritarian hacking and the frequent instances of internet manipulation or shutdown, the response “no one saw it coming” is no longer reasonable. Democracy implementers should proactively integrate cybersecurity and Internet Freedom approaches and tools into their programs, even without an obvious imminent threat. All staff have an obligation to understand the basics of cybersecurity and risks to an open internet and ensure those approaches are baked into every program, not just those specifically focused on digital threats.

Share insights on threats on the ground with donors and developers. The deep trust relationships between implementers and grassroots organizations provide the best opportunity to capture evolving cybersecurity and censorship threats, but there is little done to systematically gather or share that information. Local organizations often do not have the technical eyes to see the ways they are being targeted, and implementing organizations rarely aggregate patterns of authoritarian aggression. More frequent coordination on these topics, improvements in Internet Freedom and cybersecurity literacy by implementing organization staff, better tools for understanding and aggregating attack information, and direct connections between users and software developers can create rich feedback loops to build better tools and get them in the right hands. Implementers are often the crucial “last mile” connecting with target at-risk groups, linking distribution of and feedback about Internet Freedom tools and approaches between developers and users.

Foster a global community of Internet Freedom technologists. To understand the local context and build trusting long-term relationships there is no substitute for technologists who come from the environment in which tools are to be used. While implementers often know and work closely with a range of organizations on the ground, most are not technology-focused. Cultivating a network of tech-focused civil society organizations who are a shared resource and partner for the broader Internet Freedom community can provide local training, human-centered design expertise, and context-informed support, and can provide a pool of software developers to contribute to these tools. Many implementing organizations know individual groups around the world; by aggregating and connecting these successful technically adept partners, the

Internet Freedom community can be more robust and integrate more developer voices from the Global South.

Use secure tools beyond closing spaces. Many tools developed for risky environments have much wider utility. For example, Tella, the secure data collection app, has been used by NDI for standard election monitoring data collection. The fact that these tools are secure by design is an advantage, but additionally their mainstreaming and widespread use provides more support, a bigger user base, more real-world testing, and more funding.

Software Developers Should:

Ensure inclusion in tool development. Those most at risk online include women and marginalized communities, often bearing the brunt of censorship, surveillance, cyber attacks, and violence. However, the fact of their marginalization often means their particular needs are ignored in the development of cybersecurity and Internet Freedom tools. From problem identification to designing and scaling solutions, every step of the free, open source software development process can and should be carried out in partnership with target audiences of women and marginalized communities to develop the products they will use to achieve their goals and protect their democratic participation. The international development community is well-positioned to see that FOSS tools built with public funding are inclusive by design; in the private sector, these marginalized groups are less likely to be customers and therefore typically not a priority. As a first step, donors and implementing organizations can standardize the procurement processes for engaging in iterative user feedback and user testing with FOSS tools.

Provide training and support required to adopt new technologies. Simply having access to a new piece of software does not mean that it will be used, especially by an organization that is focused on democratic change rather than technology. This is particularly true for cybersecurity and Internet Freedom tools, which often require changing practices and organizational workflows. Most tools in this space do not have adequate documentation for non-technical users, and rarely offer technical support or even basic translation. This is an opportunity for developers to manage or partner in the support and training of their tools. Ongoing funding of tech support and training for tools could be a key aspect of the proposed Internet Freedom Infrastructure Fund.

Build components, not apps. The democracy and rights community is not burdened with the need to sell a whole tool to customers. This means developers can work on specific modular components designed to be incorporated in a wide array of products, enabling small organizations to focus on their areas of technical expertise while benefiting a much broader community of users. By incentivizing coordination, products can be brought online faster. Previous examples of sharing components include the use of the Signal encryption protocol in WhatsApp, the use of Guardian Project's obscuracam or informacam concepts in other tools, "pluggable transports" for circumvention tools, and the integration of LetsEncrypt into web server software. Similarly, specialized organizations can provide services that would be inefficient if not impossible for every Internet Freedom development team to do on their own. Localization Lab and Red Team Lab are great examples of organizations that provide critical skills by checking for security vulnerabilities and making sure tools are accessible in a range of languages and cultural contexts. Other examples of valuable services and support for organizations making tools would be human-centered design expertise, managing donor relations, or advertising and marketing, all of which could help these internet freedom developers achieve wider success and sustainability.

Conclusion

The Summit for Democracy and the Year of Action have provided a global demonstration of the political energy behind revitalizing democracy – and in the digital age, for a free, open, interoperable, and secure internet. On a much darker side, Russia's actions to limit the freedom of their own people in the wake of their unjustified and horrific invasion of Ukraine demonstrate the tremendous challenges in this space and

the urgent need for more effective approaches to keep people online. Over the last decade digital authoritarians have made frightening advances in bending the empowering vision of the early internet into an Orwellian world of computer-powered surveillance, censorship, and hacking. Dictators and autocrats in China, Russia, Iran and elsewhere have invested massively, quickly learning to take advantage of the internet's very openness to attack adversaries across the globe, chilling citizens' abilities to express themselves.

Countering authoritarian aggression requires increasing investments in internet freedom software and solving the sustainability problem through creative funding models such as the proposed Internet Freedom Infrastructure Fund. Even with effective existing Internet Freedom tools, too often at-risk groups are unaware of the threats they face and how to integrate software that can protect them into their daily work. Development implementers must be a bridge, sharing emerging threats to activists with the technical community as and tools with those at risk. The new USAID digital development strategy is an excellent start, but to follow it implementers need to make significant changes to reflect today's threats in all programs, and recognize the specific needs of the democracy community. A critical part of this role centering community-based users in tool funding and development decisions, increasing buy-in and awareness as well as connecting local democracy activists and software developers.

The Internet Freedom community also has an obligation to be more open and connected with the broader world of democracy and governance and international development writ large; a culture of secrecy designed to protect partners is at times appropriate, but makes it difficult to reach all those at risk. The democracy and Internet Freedom communities each have critical knowledge, partnerships, and commitments to building a safer world for democracy in the digital era – but in separate areas. More effective collaboration reinforced by increased resources channeled in new ways can permit these two communities to successfully confront evolving and aggressive online threats.

This is a critical moment of opportunity. Imagining a new framework for supporting democracy and human rights, empowering those using the internet to build more open societies despite the resurgence of digital authoritarians is an exciting and high-stakes opportunity for democratic leaders around the world. The international development sector has proven models to scale solutions quickly. Expansion of existing Internet Freedom funding efforts, increased coordination, and sustained support can take advantage of this moment to face the rising authoritarian threat and reinforce the system for building software that supports democracy in the digital age. With the right digital infrastructure in place, a new movement of people around the world will be able to use the power of the internet to build more open, democratic and rights-respecting societies.

References

[1] **Yayboke, Eric (March 2020). "Promote and Build: A Strategic Approach to Digital Authoritarianism". *CSIS*.**

[2] **Meserole, Chris and Polyakova, Alina (August, 2019). "Exporting Digital Authoritarianism". *Brookings*.**

[3] **Shahbaz, Adridan (2018). "The Rise of Digital Authoritarianism". *Freedom House*.**

[4] **Johnson, Joseph. (September 2021). "Internet Users in the World 2021". *Statista*. As of January 2021, active internet users account for 59.5 percent of the global population.**

[5] **Johnson, Joseph. (January 2022). "Global Internet Access Rate 2005-2021". *Statista*. The estimated annual rate of change of active internet users worldwide between 2009 and 2019 is an average increase of 2.6 percent per year**.