DEVTECH

2022

EVALUATION OF THE INTERNET FREEDOM PORTFOLIO ACTIVITIES

SUMMARY

Contract No.: 140D0421F0819

Submitted to: U.S. Department of State, Bureau of Democracy, Human Rights, and Labor

Submitted by:
DevTech Systems, Inc.
1700 N. Moore Street, Suite 1720
Arlington, VA 22209
Tel: 703-312-6038, Fax: 703-312-6039
Company Website: www.devtechsys.com

Submission Date: November 30, 2022

ACRONYMS

DOS	Department of State
DevTech	DevTech Systems, Inc.
DRL	Bureau for Democracy, Human Rights, and Labor
DRL/GP	Bureau for Democracy, Human Rights, and Labor, Office of Global Programming
EQ	Evaluation Question
FGD	Focus Group Discussion
IF	Internet Freedom
KII	Key Informant Interview
MEL	Monitoring, Evaluation, and Learning
SME	Subject Matter Expert

DEFINITIONS OF KEY CONCEPTS

Internet freedom: The "expression of human rights online, Internet governance consistent with democratic values and human rights norms (open, interoperable, secure, and reliable), protection for civil society, and vulnerable populations online."[1]

Effectiveness: The extent to which established objectives are met, program goals are explicitly pursued, and program values are followed.

Illicit use: An action or activity performed by an individual, group, or organization that is considered to be criminal in nature according to U.S. or international law and/or "that reflect(s) any type of support for any member, affiliate, or representative of a designated terrorist organization."[2]

Safeguards to prevent illicit use of tools: A programmatic strategy—based on the orientation and focus of the program —for preventing or making less likely the illicit use of IF-funded tools. It can include the application of a human rights frameworks to programming (e.g., human rights-centered design) and thus a focus on (1) identifiable organizations that work with targeted beneficiaries among human rights defenders, journalists, civil society, and members of marginalized or vulnerable populations, and which are far less likely to practice or facilitate illicit use, (2) the application of proposal and program review controls that reduce the likelihood of illicit use opportunities and identify questionable activity when it is discovered, and (3) the periodic external evaluation of the illicit use mitigation strategy.

[1] Internet Freedom, Strategic Framework 2021

[2] Internet Freedom, Request for Statements of Interest: DRL FY22 Internet Freedom Annual Program Statement. state.gov/request-for-statements-of-interest-drl-fy22-internet-freedom-annual-program-statement/

Background

The United States Department of State (DOS), Bureau for Democracy, Human Rights, and Labor, Office of Global Programming (DRL/GP) commissioned DevTech Systems, Inc. (DevTech) to conduct a mixed method evaluation of the Internet Freedom (IF) Portfolio to examine the effectiveness of its strategy; garner lessons learned; assess progress; and ascertain any unintended outcomes, whether positive or negative. This summary presents a snapshot of the evaluation team's evidence-based findings and conclusions as well as action-oriented recommendations for DRL/GP's consideration.

The IF Portfolio is built upon DRL/GP's IF Strategic Framework. The Framework is organized along four overarching pillars. Each pillar contains several lines of effort, or areas of focus, to which individual programs respond. In the period covered by this evaluation (2015–2021), the IF Portfolio implemented 88 programs across 14 lines of effort under the four pillars. Employing a purposive (i.e., non-random) sampling approach, this evaluation assessed the outcomes of 16 programs pre-selected by DRL/GP. The 16 pre-selected programs covered nine of the 14 lines of effort (bolded below in Figure 1) yet spanned all four pillars.

Figure 1. IF Strategic Framework

Pillar	Technology Development	Digital Safety	Policy Advocacy	Research
Goal	To support the development of technologies that provide or enhance access to the Internet, including circumvention tools that bypass Internet blocking, filtering, and other censorship techniques used by authoritarian governments.	To enhance digital security training and capacity building for democracy activists and to combat violence against bloggers and other users.	To support the efforts of civil society to counter the development of repressive Internet-related laws and regulations, including countering threats to Internet freedom at international organizations.	To research key threats to Internet freedom.
Line of Effort	**1. Anti-Censorship Tech** **2. Secure Communications** 3. Peer-to-Peer Communications **4. DDOS Mitigation** 5. Small Grants	**6. Digital Security Capacity-Building.** **7. Emergency Support** **8. Public Awareness-Raising & Education**	**9. Human Rights in Internet Policy** 10. Internet Freedom in Human Rights 11. IF / Business & Human Rights **12. Legal Advocacy**	**13. Global Rankings** **14. Censorship Measurement**
	Public Awareness Raising – Cross Cutting			

Evaluation Purpose

The purpose of this evaluation was to provide DRL/GP and the IF team with findings and conclusions to better understand the effectiveness of their current programming strategies and to identify achievements at both the output and outcome levels. The evaluation team assessed the extent to which the IF Portfolio minimized the risk of unintended negative outcomes yet maximized unexpected or unintended opportunities that emerged. In addition, the evaluation team explored and captured useful implementation lessons learned that can be applied in future programming. The recommendations will support DRL/GP and IF in determining which implementation strategies should be continued, discontinued, or adapted moving forward to facilitate success in meeting its objectives, while minimizing the use of IF-funded technologies for illicit purposes or use. In addition, the evaluation team has generated data on the IF Portfolio and the extent of its effectiveness in advancing human rights and fundamental freedoms, including Internet freedom, to be disseminated among a broader audience.

To meet the objectives of the evaluation, the evaluation team answered the following evaluation questions (EQs).

1. **Effectiveness:** How effective are IF Programs completed within the last five years, as assessed against the IF Strategic Framework indicators, values, and goals?
2. **Accuracy and Relevancy:** How accurate are the assumptions that form the basis of the IF Strategic Framework Lines of Effort?
3. **Safeguards:** How have DRL's current safeguards been successful in minimizing the use of IF-funded technologies developed within the Technology Development Pillar for illicit purposes, considering the risks and benefits of those safeguards to the IF Program's ability to meet the objectives, goals, and values in the IF Strategic Framework?

Methodology

DevTech utilized a mixed-method approach integrating qualitative and quantitative approaches to data collection to answer the three EQs. A combination of desk and literature research, key informant interviews (KIIs), focus group discussions (FGDs), discussions with independent subject matter experts (SMEs), and a stock-taking characterization exercise, which included an anonymous online survey, expert panel, and a case study of safeguards, were used to gather relevant data from multiple stakeholders. By drawing on diverse data sources and data types, the evaluation team triangulated data across multiple sources to verify findings, increasing the reliability of the findings and resulting conclusions and recommendations.

Key Findings

DRL/GP's IF portfolio has and continues to serve a critical role in promoting human rights online through its programs focused on developing and enhancing technologies (Pillar 1), equipping digital activists and human rights defenders to combat digital attacks (Pillar 2), empowering civil society to challenge repressive laws and policies (Pillar 3), and expanding the existing evidence base with cutting edge research on Internet freedom-related challenges (Pillar 4). Through their various programs, DRL/GP is filling a critical void within the broader ecosystem. Stakeholders alike emphasized that, "if not for DRL, [and] the overall U.S.

government commitment… to internet freedom, we would probably be in a much worse situation than we are today." Another independent SME further noted, "this is really an area where DRL is providing a central support…, that, in the absence of the level of funding from the U.S. government and from DRL, in particular, we would be in a very different place than if [these] programs did not exist."

PILLAR 1: TECHNOLOGY DEVELOPMENT

The Technology Pillar's goal is to support the development of technologies that provide, or enhance, access to the Internet by providing circumvention tools that bypass blocking, filtering, and other censorship techniques used by authoritarian governments. As demonstrated by the effective progress against the pillar's indicators and values, DRL/GP's approach—supporting a plurality of tools—has been and will continue to be an integral part of its success, mitigating the sudden elimination or blocking of a specific tool. However, while often creating redundancy and resiliency for the whole system, it is important to also be mindful that the sheer number of technologies in the Internet freedom space, can also create challenges for end users and sustainability issues for developers.

Some interviewed stakeholders, in speaking to transaction costs of technology adoption, described the complexity regarding choice of technology and learning curve for their effective use. From the developer perspective, it can be challenging to obtain sustained funding to consolidate and expand on the success of pilot technologies and to develop and release necessary updates that deal with new challenges. Moreover, some societies still limit the ability of a user—the intended beneficiary—to even access those solutions in the first place. Thus, a holistic approach to technology development that considers the context of the user at a macro and micro level, as reflected by DRL/GP's strategy and corresponding theories of change, is desirable.

In that vein, the value of user-centered design emphasizes "building with, not for" the intended end users and developing tools that prioritize usability. As one interviewed stakeholder summarized, "no matter how secure [the technology] is, if it's not easy to use, then people are not going to use it or they're not going to use it properly." For many of the sampled grantees, effectively fulfilling the value of user-centered design rested in large part on collecting feedback from and working directly with end users.

> "We brought the domain developer to one of our first tool feedback sessions. And he was able to see that users refused to use [the encrypted email tool] because there was no way for them to send encrypted attachments. The developer quickly realized that if that workflow was not available, then this was not a tool for them. And so the lead developer took that feedback, and shortly released a new version which included that feature. So it was a direct result of [engaging with users] and witnessing users select other tools because of the limited functionality."
>
> DRL/GP Grantee

SAFEGUARDS

While IF-funded technologies are designed to enhance the privacy and anonymity of human rights activists, journalists, individuals in countries with highly oppressive regimes, minorities, and vulnerable groups so they

can continuously exercise and defend human rights and fight for democratic values; there is a need to ensure that mitigation strategies are in place to deter the potential illicit use of technologies and related tools. For example, anti-censorship and privacy protecting technology could also help certain actors "to conceal or commit illegal activity" and even present a threat "to other aspects of … national security." [1]

From the onset, DRL/GP successfully laid a strong foundation to prevent risks of illicit use of IF-funded technologies. The safeguards established in the DRL/GP Illicit Use Mitigation Strategy—notably, the application of a human rights framework and proposal and project review controls—are the strongest ones in the broader Internet freedom ecosystem to prevent risks of illicit use technologies. By anchoring technology design in the unique needs of human rights defenders and vulnerable populations as compared to the quite different needs of criminals, the human rights use case sets a solid and cohesive filter to select technologies with the lowest risk of being used illicitly.

Moreover, the established safeguards support the promotion of the DRL/GP's broader IF goals and values. However, an opportunity exists to enhance and further the success of DRL/GP-funded technologies by enhancing and building upon the existing safeguards to mitigate illicit use. Nevertheless, no major illicit uses of DRL/GP-funded technologies were found or disclosed within the evaluated grants.

> "Targeting the Human Rights use case, and specifically communities of need, is an effective method for making sure that illicit actors do not use the technology, [yet] it is not an absolute guarantee that no one will ever do that. But it is an effective mitigation against illicit use. I think that when you build things for people who are suffering under repression of human rights, they tend to use it, they tend to be the beneficiaries, it tends to stay, and be used among communities of need. [And,] that is a very effective way to target your impact. Whereas criminals have a tendency to use other things."
>
> DRL/GP Representative

PILLAR 2: DIGITAL SAFEGY

The goal of the digital security pillar is to enhance digital security training and capacity building for democracy activists and to combat violence against bloggers and other users. User-generated content has shifted from primarily being self-hosted on blogs to being hosted and shared on and through a variety of different platforms. Because of this, the word bloggers should be interpreted broadly to include any Internet user. The evaluation found that the sampled grants effectively pushed forward on this goal building upon the established theories of change that accurately reflect the historical and evolving nuances of digital security, emergency support, and public awareness raising within the ecosystem. Notably, localized solutions were found to have contributed to and enhanced DRL/GP's approach and subsequent success around digital safety. Several grantees set up local resources as part of their activities, directly connecting to the values of time-sensitive response to attacks and addressing the security needs of vulnerable populations online. As one stakeholder reflected, local support solutions help "to focus on realistic threats and realistic attacks that are pertinent to […] a human rights defender, a targeted minority group, whatever the case may be," and to begin to develop data-driven solutions specific to those groups.

However, while DRL/GP's overarching IF Strategic Framework demonstrates its' commitment to a holistic, systems-based approach, the respective theories of change that inform DRL/GP's digital safety programs could benefit from further emphasis on these principles. Moreover, as one independent SME pointed out, "if you do not support digital security training for everybody, you are actually creating [additional risks], if only the activists are using certain tools, they are very easy to spot. You almost have to hide them within a greater amount of noise to make sure everybody is using those tools."

PILLAR 3: POLICY ADVOCACY

The Policy Advocacy pillar's goal is to support civil society to counter the development of repressive Internet-related laws and regulations, including countering threats to Internet freedom at international organizations by, in part, advocating for human rights in Internet policy and challenging repressive laws that restrict freedom of expression online. As evidenced by the effective progress against the pillar indicators and values, the sampled grants were successful in pushing towards this goal.

Furthermore, the theories of change and underlying assumption which inform the DRL/GP Policy Advocacy Pillar, accurately reflect the historical and evolving nuances of challenging repressive Internet-related laws and regulations within the Internet freedom ecosystem. Notably, DRL/GP's multi-stakeholder approach empowered a diverse network of civil society to serve as champions contributing to tangible improvements to repressive laws, policies, and procedures. While glimmers of success have emerged, due to the nature of this work, the full impact of DRL/GP's policy advocacy efforts will only be realized over time.

> "DRL is basically the only donor in the world to invest in this. So if anything good has happened in the last 10 years around this, DRL should be the one who gets credit. There have been huge wins in this space just in terms of representation of these issues, and with civil society, leading them across a number of international governance bodies as well as technical standards setting bodies."
>
> Independent SME

PILLAR 4: RESEARCH

Ultimately, the goal of the Research Pillar is to research key threats to Internet freedom. As the findings demonstrate, the sampled grants effectively pushed this goal forward, delivering timely and relevant information to stakeholders about core Internet freedom issues. IF-funded research initiatives under this pillar fill an existing void, contributing to the development of metrics for assessing laws, policies, and procedures that respect human rights online.

Specifically, the uptake of the produced methodologies and associated research products illustrate the advancement of this goal. Research, standards setting, and normative assessments have helped to "change the landscape overall in terms of setting expectations for what our rights should be and how they should be realized."

Furthermore, the Global Ranking's theory of change along with its underlying assumptions accurately reflect the historical and evolving nuances surrounding the Internet freedom ecosystem, thus advancing the available research and existing evidence base.

Recommendations

While the Internet freedom ecosystem has developed extensively over the past decade—in part due to DRL/GP's programs, contributing to a well-established ecosystem—the ecosystem continues to rely heavily on DRL/GP funding to propel technology development, digital safety, policy advocacy, and research forward. To maintain forward motion and to ensure that DRL/GP remains a leader in Internet freedom, the evaluation team suggests that DRL/GP consider the following key recommendations.

1. **Sensitize grantees, among other key stakeholders across the Internet freedom ecosystem, on key terms and concepts of DRL/GP's vision for success.** Moving forward, DRL/GP could consider reflecting upon the existing theories of change and underlying assumptions to provide public facing definitions for key terms.

2. **Consider formalizing an overarching IF Monitoring, Evaluation, and Learning plan**. Despite having a clear set of IF Strategic Framework Indicators, tailored to each of the respective pillars, grantees did not consistently embed these indicators into their grant MEL plans and thus did not report performance against these indicators. To address these limitations, the evaluation team suggests that a MEL plan be formalized, to clearly outline the requirements for grantees including examples of data sources, data collection requirements, and reporting frequencies, among other key concepts and best practices in monitoring program effectiveness. Following the completion of data collection, the evaluation team discovered that DRL/GP has already taken steps to move forward with developing and formalizing a plan to address these concerns.

3. **Conduct a gap analysis** to expand the IF Strategic Framework to address funding gaps and needs within the ecosystem to further Internet freedom. The evaluation team suggests that DRL/GP consider conducting a gap analysis of the ecosystem broadly, to better understand the funding needs of marginalized and vulnerable populations considering the role of other donors and funders to reduce duplication of efforts while maintaining saturation of support for communities at large.

4. **Continue to review and update theories of change** to reflect the ever-evolving context of the Internet freedom ecosystem.

5. **Update and expand the IF Illicit Use Mitigation Strategy** to more clearly articulate the process that is implemented throughout the grant cycle. In addition, the Strategy should be updated to allow external evaluators and grantees the opportunity to fully understand how risks and safeguards are identified.

6. **Intentionally and strategically collaborate with grantees under Pillar 1** to enhance the effectiveness of safeguards to mitigate illicit use. Defining illicit use and safeguards as noted above is an important step in strengthening grantees' capacity to mitigate illicit use. Furthermore, outside of DRL/GP's independent risk assessments, upon award, DRL/GP may consider engaging grantees more actively to enrich the process and equip DRL/GP to tell a more complete story on the effectiveness of their efforts under Pillar 1.

[1] Fontaine, Richard and Rogers, Will. (2011). Internet Freedom: A Foreign Policy Imperative in the Digital Age. Center for a New American Security. https://www.files.ethz.ch/isn/129550/CNAS_InternetFreedom_FontaineRogers_0.pdf