DEVTECH

2022

EVALUATION OF THE INTERNET FREEDOM PORTFOLIO ACTIVITIES

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 29, 2022

Contents

TABLE OF FIGURES

TABLE OF TABLES

ACRONYMS

COR	Contracting Officer's Representative
DOS	Department of State
DDOS	Distributed Denial of Service
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
ET	Evaluation Team
FGD	Focus Group Discussion
FOTN	Freedom on the Net
HR	Human Rights
HRIA	Human Rights Impact Assessment
IF	Internet Freedom
KII	Key Informant Interview
LGBT	Lesbian, gay, bisexual, and transgender
MEL	Monitoring, Evaluation, and Learning
MENA	Middle East and North Africa
NEA	DOS Bureau of Near Eastern Affairs
OTF	Open Technology Fund
SFOPS	Department of State, Foreign Operations, and Related Programs
SME	Subject Matter Expert
UPR	Universal Periodic Review
USAGM	U.S. Agency for Global Media
USAID	United States Agency for International Development
VPN	Virtual Private Network

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.

EXECUTIVE SUMMARY

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. As a result of these efforts, this report presents the evaluation team's evidence-based findings and conclusions as well as action-oriented recommendations for DRL/GP's consideration.

Evaluation Purpose

The purpose of this evaluation report 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 in this report 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 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-methods 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. The methodology and corresponding data collection methods and analytic approaches are described in detail in Annexes 2 and 3. The desk and literature review is then provided in Annex 4. 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 presented in this evaluation report.

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."[3] 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."[4]

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. 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.

SAFEGUARDS

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.

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. 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.

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.

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. Specifically, the uptake of the produced methodologies and associated research products illustrate the advancement of this goal. 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.
2. Consider formalizing an overarching **IF Monitoring, Evaluation, and Learning plan**.[1]
3. Conduct **a gap analysis** to expand the IF Strategic Framework to address funding gaps and needs within the ecosystem to further Internet freedom.
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.
6. Intentionally and strategically **collaborate with grantees under Pillar 1** to enhance the effectiveness of safeguards to mitigate illicit use.

[1] 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.

INTRODUCTION

Many citizens across the globe often face legal and technology restrictions that limit their ability to access information and to articulate their thoughts, ideas, and opinions without fear of surveillance, reprisal, or violence. This is especially true in countries where there are severe or emerging restrictions on the rights of freedom of expression, assembly, and privacy. In response, the United States Department of State (DOS), Bureau for Democracy, Human Rights, and Labor, Office of Global Programming (DRL/GP) launched the Internet Freedom (IF) Portfolio. The IF Portfolio was designed to advance human rights, including Internet freedoms, in accordance with the mandates of the Consolidated Appropriations Act and U.S. National Cyber Strategy, notably in those countries where severe or emerging restrictions threaten citizens' abilities to exercise their rights to access the global Internet and communicate their thoughts, ideas, and opinions freely. To date, the IF Portfolio has supported over 150 programs, of which over 50 remain active, in every region of the world.

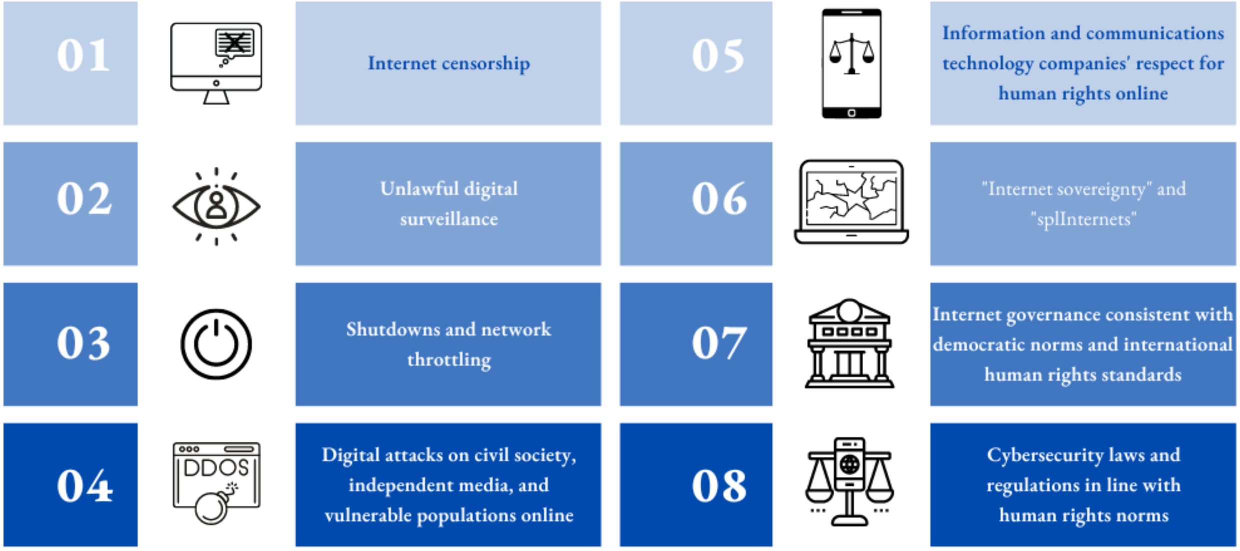
DRL/GP commissioned DevTech Systems, Inc. (DevTech) to conduct an evaluation of the IF Portfolio to (1) examine the effectiveness of IF's overarching strategy and current programming in meeting its established objectives and goals; (2) garner important implementation lessons learned that can be applied to future programming; (3) assess progress at the output and outcome levels; and (4) ascertain any unintended outcomes, whether positive or negative, resulting from programming. To inform this evaluation and address the evaluation questions (EQs), the evaluation team conducted both primary and secondary research to collect qualitative and quantitative data. The research methods included a desk and literature review, secondary data analysis, in-person and virtual semi-structured key informant interviews (KIIs), virtual focus group discussions (FGDs), individual discussion with SMEs, a characterization exercise, and a panel of experts. As a result of these efforts, the report presents the evaluation team's evidence-based findings and conclusions as well as action-oriented recommendations for DRL/GP's consideration.

Background and Understanding

DRL identified three areas of focus related to Internet policy—Infrastructure, Internet Freedom, and Content and Information on the Internet—that reflect a multi-agency effort to address U.S. Government priorities on this critical issue.[5] As outlined in the 2015–2021 DRL Functional Bureau Strategy,[6] the U.S. President's National Cyber Strategy,[7] and U.S. federal consolidated appropriations legislation,[8] the DRL/GP IF Portfolio responds to the second of these three policy areas: Internet Freedom. The Internet Freedom policy area includes activities related to the exercise of human rights online, Internet governance consistent with democratic values and human rights norms, and protection for civil society and vulnerable populations online. The Internet Freedom policy area does not address the availability of Internet infrastructure, nor the content disseminated on the Internet, but addresses, through programming, Internet freedom, recognizing the element as essential to the success of the other policy areas.

Specifically, the IF Portfolio aims "to protect the open, interoperable, secure, and reliable Internet by promoting fundamental freedoms, human rights, and the free flow of information online through integrated support to civil society for technology, digital safety, policy and advocacy, and applied research programs."[9] Managed by DRL/GP, by funding active programs in every region of the world, IF seeks to counter the efforts of authoritarian regimes that censor, monitor, and control the Internet, focusing on countries where there are severe or emerging restrictions on freedom of expression, assembly, or privacy online. To this end, the IF Portfolio is designed to address the following key "problem areas":[10]

Figure 1. Key Problem Areas



01 Internet censorship

02 Unlawful digital surveillance

03 Shutdowns and network throttling

04 Digital attacks on civil society, independent media, and vulnerable populations online

05 Information and communications technology companies' respect for human rights online

06 "Internet sovereignty" and "splInternets"

07 Internet governance consistent with democratic norms and international human rights standards

08 Cybersecurity laws and regulations in line with human rights norms

These key problem areas and the contexts in which they are found are rapidly evolving. The challenges, risks, and opportunities facing the IF portfolio's target populations—including "individual citizens, activists, human rights defenders, independent journalists, civil society organizations, and marginalized populations"[11]—are complex and dynamic.

Evaluation Purpose and Approach

The purpose of this evaluation report is 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. Additionally, and within the mandate, 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. Finally, the evaluation team also explored and captured useful implementation lessons learned that can be applied in future programming. The report ends with a set of recommendations to 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. To support the recommendations, 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, that can be disseminated among a broader audience.

Evaluation Methodology

To meet the objectives of the evaluation, the evaluation team answered the following 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?

a. Which safeguards have not been effective among these?
b. What are other effective safeguards that the DRL IF team should consider utilizing to minimize IF-funded technologies for illicit purposes?

DATA COLLECTION METHODS

The DevTech evaluation team utilized a mixed-methods approach integrating qualitative and quantitative approaches to data collection to answer the three EQs. A combination of desk and literature research, KIIs, FGDs, discussions with independent 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. The evaluation methodology and corresponding data collection methods and analytic approaches are described in detail in Annexes 2 and 3. The desk and literature review is then provided in Annex 4. By drawing on diverse data sources and data types, the evaluation team triangulated data across multiple sources to verify findings thus increasing the reliability of the findings and resulting conclusions and recommendations presented in this evaluation report.

SAMPLING

To answer the EQs, the evaluation team conducted a purposive (i.e., non-random) sample of DRL/GP's IF Portfolio team members, implementing partners/grantees, independent SMEs, and a panel of outside experts. The sampling strategy aimed at capturing a diversity of points of view. The evaluation team's sampling approach also drew upon snowball sampling to reflect learning throughout the data collection process. A snowball sampling approach occurs when researchers begin with a small sample of informants who meet an established criterion and over time, researchers expand the sample size based on recommendations provided by the existing pool of informants of other experts to engage. Please refer to Table 1 for a summary of data collected across the target sample group.

Table 1. Data Collection by Pillar

Stakeholders	Pillar 1	Pillar 2	Pillar 4	Pillar 3
Implementing Partners	4	7	3	2
Subject Matter Experts	7	3	9	4
DRL/GP IF Portfolio Team Members	4	3	2	2
DRL/GP IF Portfolio Leadership	1	1	1	1
Total	16	14	14	9

DATA ANALYSIS

The evaluation team drew on various analytical tools to inform the three EQs. Evaluation team members transcribed and cleaned KII and FGD notes on a rolling basis throughout fieldwork. Team members conducted periodic internal debriefs to identify trends and begin formulating preliminary findings. To reduce potential cognitive bias in the research and ensure the evaluation findings' validity and reliability, the evaluation team coded trends and results to crosscheck and systematically triangulate the findings against multiple data sources. Additionally, through coding and cleaning the evaluation data, the evaluation team maintained respondent anonymity. The following summarizes the analytical approaches for each of the respective EQs.

- To inform EQ 1, the evaluation team analyzed the data drawing on the systematic approach of Secondary Analysis combined with Thematic and Content Analysis. Following the completion of KIIs and FGDs, the evaluation team categorized and coded qualitative data to assess the perceived levels of success of the IF Portfolio against the Strategic Framework. Using the interview and FGD transcripts, as well as the available secondary, quantitative data reported by DRL/GP's implementing partners, the team then produced case studies that speak to the objectives, goals, and values in the IF Strategic Framework.

- To answer EQ 2, the evaluation team analyzed the cause-effect relationship to understand what outcomes the line of efforts were intended to achieve and how (by what mechanisms). The team developed a preliminary Contribution Story to assess the plausibility of alternative explanations to check whether the desired results could have plausibly been generated by other mechanisms external to the program. In addition to using trend analysis and divergence/convergence analysis to assess the relevant KIIs and FGDs, this exercise consisted of studying historical, economic, and policy-specific factors related to obstacles to Internet freedom. The evaluation team then formulated a revised Contribution Story, reassessing the theories of change against evidence to produce a narrative of cause and effect and situate it in the realm of alternative causal explanations.
- To inform EQ 3, the evaluation team first identified the general and specific safeguards the IF Portfolio had in place in its programmatic strategy to prevent and mitigate illicit use of the technologies it supports. Then, identifying the risks and benefits of those safeguards by means of the literature review, the evaluation team developed an online survey and characterization exercise. The evaluation team systematized the quantitative data from the survey to pinpoint which safeguarding measures are more and less effective and cross-tabulate them by type of technology, geographic area, relative risks, benefits, grantee, and other variables of interest. Then, based on the follow-up interview transcriptions, the team produced unique case studies that speak to the objectives, goals, and values of the IF Portfolio.

LIMITATIONS

Limitation of Cognitive Bias. Key informants and FGD participants constitute a key source for answering all three EQs, but interview data is also prone to cognitive biases, including recall and social desirability. To mitigate the potential cognitive bias, the evaluation team began each KII and FGD with a protocol that reviewed IF's objectives and explained the evaluation purpose and how the data would be used and confidentiality ensured. In addition, with respect to EQ 3—the effectiveness of the established safeguards, the evaluation team shared the DRL/GP's definition of illicit use and provided a brief overview of the established Illicit Use Mitigation Strategy prior to the discussion. Individual responses were organized by EQ and coded to reveal trends across respondents within a similar group. The evaluation team then assessed key trends across respondent groups to generate preliminary findings. To ensure the evaluation's validity and reliability, the team systematically triangulated data across respondent groups as well as data-collection methods, using multiple data sources to identify whether and where there is alignment or divergence in findings, to generate actionable conclusions and recommendations.

Limitations to Organizing KIIs and FGDs. The challenges associated with in-person qualitative data collection being replaced by remote data collection are diverse. Remote KIIs and FGDs do not allow for the same rapport building that in-person interviewing makes possible. Unobtrusive observation was also not possible. To mitigate this limitation, the evaluation team carried out online KIIs and FGDs in a way that allows for asking open-ended questions. The evaluation team also offered opportunities for a more in-depth discussion about specific points related to the implementation of IF programs and the results achieved.

Online Survey Risks of Low Response. While electronic surveys can reach large numbers of respondents, the challenge is often low uptake and the inability to ask probing questions. The evaluation team worked with DRL/GP at the beginning of the evaluation, leveraging DRL/GP's existing relationships to inform all potential respondents of the purpose and importance of the evaluation and the anonymous nature of the survey. In an effort to increase uptake and response rates, DevTech also used an online automated survey platform, Survey Monkey, that tracks response rates and sends respondents reminder emails if they have not yet completed the survey.

STRATEGIC FRAMEWORK

The IF Portfolio is built upon DRL/GP's IF Strategic Framework. The Framework itself 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, however, assessed the outcomes of 16 programs, pre-selected by DRL/GP. The 16 pre-selected programs covered nine of the 14 lines of effort yet spanned all four pillars to inform each of 3 EQs (bolded below in Figure 2).

Figure 2. IF Strategic Framework[12]

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 organizati ons.	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**
Portfolio	22 Active Programs valued at USD 29.85 million	23 Active Programs valued at USD 16.04 million	Nine Active Programs valued at USD 6.4 million	2 Active Programs valued at USD 2 million

Public Awareness Raising – Cross Cutting

IF Framework Alignment with Strategic Policies

The IF Portfolio demonstrated clear and close alignment with other DRL and U.S. Government strategic policies and guidelines.

- **DRL Functional Bureau Strategy.** The DRL Functional Bureau Strategy contains two objectives most pertinent to the IF Portfolio. These are: (1) *Bureau Objective 2.1*: Support and enhance the capacity and impact of independent journalists, civil society, and political parties to maximize openings of political space and demand democratic, accountable governance, including using an open and interoperable Internet; and (2) *Bureau Objective 3.4*: Build the capacity of democracy advocates, independent media, and civil society representatives to promote human rights and hold their own governments accountable for human rights violations.[13]

  The IF Strategic Framework's pillars of technology development, digital safety, policy advocacy, and research, as well as the cross-cutting priorities of education, capacity building, and tailored local solutions reflected in the IF Strategic Framework's values, goals, and individual programs, **strongly align with these DRL Functional Bureau Strategy objectives**. Numerous grants included training and capacity building components through the delivery of training seminars, hosting conferences, or developing and publishing content for asynchronous use by end users. The emphasis on localized solutions within the IF Portfolio aligns with the Functional Bureau Strategy objectives by **promoting the relevance—and thus the uptake and sustained usage—of the intervention**. For example, applications and other technology solutions supported by the IF Portfolio were routinely made available in different languages, designed to function on diverse operating systems, and made compatible with basic smart phones, to name a few examples. The model used in one of DRL/GP's Policy Advocacy projects (Policy Advocacy Project B) reflects principles found across the IF Portfolio to deliver tailored tools and capacity development to diverse stakeholders to facilitate advocacy efforts—directly aligning with *Bureau Objectives 2.1 and 3.4*. The models provided a space for local groups to develop IF-relevant policy and technology innovation in a series of local, competitive incubation events to design interventions, compete for small grants, and receive relevant topical training.

- **National Cyber Strategy.** The IF Portfolio directly aligns with Pillar IV (Advance American Influence) of the National Cyber Strategy—namely, the objective to promote an open, interoperable, reliable, and secure Internet. Two priority actions within this objective directly link to the IF Portfolio: (1) to protect and promote Internet freedom and (2) to work with like-minded countries, industry, academia, and civil society toward this end.[14] As discussed above, the IF Portfolio's emphasis on technology development, capacity building, and tailored local solutions that engage diverse stakeholders directly align with these aspects of the National Cyber Strategy. Pillar III of the National Cyber Strategy centers on the development of a superior cybersecurity workforce. This pillar emphasizes the importance of a skilled American cybersecurity workforce as a "strategic national security advantage" and further emphasizes the need to attract those "who share our values." It is not within DRL/GP's purview to engage in programming that supports the development of a cybersecurity workforce within the United States. However, it is within the IF Portfolio to fund work to engage, educate, and build the capacity of diverse stakeholders around the world—those "who share our values"—to engage in Internet freedom work and deliver localized cybersecurity solutions. For example, a DRL/GP-funded technology (Technology Project C) upskilled 59 digital security trainers from 26 countries, enabling skilled support to be delivered to 480 at-risk end users.[15]

  From a broader lens, the IF Portfolio further provides—through its grants—opportunities for implementers to engage highly skilled cybersecurity personnel "who share our values" and prolong their involvement in programming supportive of U.S. interests. That said, most interviewed grantees cited the challenge of obtaining ongoing funding and a vocal minority shared that "there are not mechanisms for retaining [specialized staff] long term; there is not funding to give them half of what they could make in the private sector."[16] Interviewees further linked this challenge to the prioritization by nearly all donors of finding novel technological solutions rather than continuing to fund proven technologies. Prioritizing innovation is another priority action in the National Cyber Strategy (under the Pillar II objective to foster a vibrant and resilient digital economy). As interviewees noted, however, this may compound pre-existing challenges sustaining successful technology as well as the careers of specialists "who share our values."

- **Interim National Security Strategic Guidance.** The enumerated national security priorities include "prevent[ing] adversaries from […] inhibiting access to the global commons or dominating key regions" and to "lead and sustain a stable and open international system, underwritten by strong democratic […] rules."[17] The concept of Internet freedom, particularly the online exercise of human rights and fundamental freedoms, directly aligns with the national security priority of protecting access to the global commons. The IF Framework's digital security and policy advocacy pillars further promote democratic rules to access, contribute, and participate in this "global commons" online by building the capacity of, supporting, and actively protecting human rights advocates.

Impact of DRL/GP Internet Freedom Programming

The IF Portfolio and its programs have contributed to the overarching IF Strategic Framework—particularly the Framework's values and goals—supporting the development and enhancement of the Internet freedom ecosystem.

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."[18] Another independent SME further noted, "this is really an area where DRL is providing 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."[19]

The following sections provide a snapshot of the impact of DRL/GP funding across each of the four pillars as assessed by this evaluation, including its effectiveness (EQ 1) and the accuracy and relevancy of the respective theories of change and underlying assumptions which comprise the framework (EQ 2). Furthermore, with respect to technology development, the Safeguards section highlights the success of DRL/GP efforts to mitigate the potential use of its supported technologies for illicit purposes (EQ 3). Based on these findings, the evaluation team presents a series of actionable recommendations for DRL/GP consideration to further enhance the IF Strategic Framework, thus extending the impact of its programs

PILLAR 1 TECHNOLOGY DEVELOPMENT

The first pillar within IF's Strategic Framework is the Technology Development Pillar, through which DRL/GP aims to improve Internet freedoms and advance human rights by supporting 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...."[20] To achieve this goal, DRL/GP established five core lines of effort through which it supports the development and deployment of circumvention tools that bypass Internet blocking, filtering, and other censorship techniques as well as technology to secure activists in surveillance environments and protect them against distributed denial of service attacks.

THEORIES OF CHANGE AND UNDERLYING ASSUMPTIONS

The Technology Development Pillar is comprised of five lines of effort: (1) Anti-Censorship Technology, (2) Secure Communications, (3) Peer-to-Peer Communications, (4) DDoS Mitigation, and (5) Small Grants. Of these five, only three—Anti-Censorship Technology, Secure Communications, and DDoS Mitigation—were included as part of the evaluation per DRL/GP guidance. To assess the effectiveness (EQ 1) and relevancy (EQ 2) of DRL/GP's efforts related to these lines of effort, it is imperative to first understand the perceived pathway of change or theory of change describing how and why a specific or set of interventions are believed to contribute to the desired goal or end result. In addition, it is likewise just as important to understand the underlying assumptions within a given theory of change. Underlying assumptions provide a clear picture of the conditions and resources required for change to occur. Please refer to Annex 5 for DRL/GP's Technology Development Theories of Change and identified underlying assumptions.

EFFECTIVENESS OF PILLAR 1

Effectiveness Towards IF Framework Indicators

The technology development pillar largely tracks output level indicators, including the number of tools supported by DRL/GP, average unique monthly users of those tools, and contributions made by external actors. Although none of the sampled grants reported on the third indicator, they were highly effective when assessed against the first two indicators.

DRL/GP SUCCESSFULLY SUPPORTED THE DEVELOPMENT OF

12

UNIQUE TOOLS ACROSS 4 GRANTS UNDER PILLAR 1

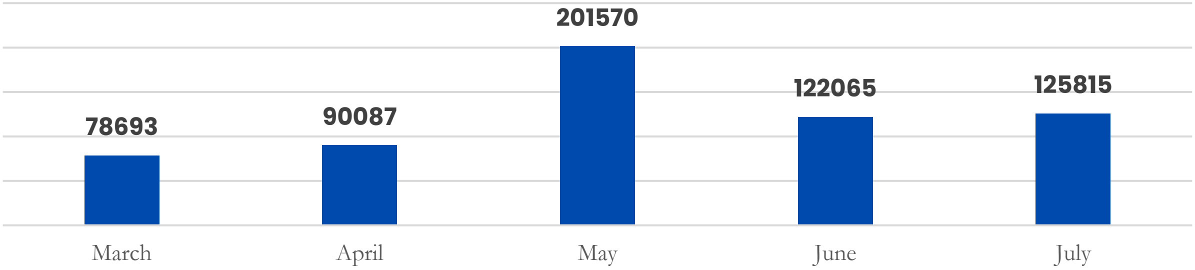
DRL/GP has supported the development of a variety of technologies, reaching an impressive number of monthly users to combat restricted access and promote surveillance free communication.

Indicator 1.1-1. Number of tools supported by the DRL Internet (IF) award. Within the sampled grants, the IF Portfolio supported numerous diverse tools. Technology

Projects A and B supported one anti-censorship technology each, for a total of two. Through Technology Project C, IF supported eight open-source privacy and security tools.[21] Under Technology Project D for DDoS mitigation, IF funding supported the improvement of an existing system and a new early warning system drawing data from the existing system.[22]

Indicator 1.1-2. Number of average unique monthly users of DRL IF supported tools. Trends in average monthly users serves as a proxy to measure sustained demand for that technology.[23] The sampled grants successfully reached significant numbers of monthly users during the grant period and—in some cases—available information indicates continued growth in usage after the conclusion of the grant. Technology Project B, for example, demonstrated overall positive growth in average monthly users. An example in one of the target countries demonstrates the use and relevance of the technology developed under this grant. After being blocked, an independent publication "utilized [the technology] to continue delivering their content and since then its audience has grown" from approximately 250,000 users "to 2 million over a couple of weeks. It is particularly interesting that a very small, non-tech organization was able to use [the] tool as it was straightforward to use."[24]

Figure 2. Number of Unique Monthly Users, 2021[25]



Technology Project A provides the opportunity to review the effectiveness of the grant against this indicator as well as its sustainability and expansion since DRL's investment. The grantee reported a 104 percent increase in average daily downloads following their release of the VPN; download spikes corresponded with periodic campaigning efforts but overall, downloads for the browser and VPN "settled at a level of roughly double the level of browser-only downloads."[26] In total, the grantee documented approximately 1.8 million downloads during the course of the grant. Usage of Technology Project A's tool has continued to grow since the end of the grant period, with an estimated average monthly rate of 35 million users. [27] Furthermore, the technology was described by external stakeholders as reflecting an increasing level of autocratic controls in countries. When other technologies are blocked by host governments, Technology Project A's tool is able to break through the firewalls, providing solutions in diverse and challenging environments, such as China, Russia, Cuba, Saudi Arabia, and others, to access information securely.[28] Notably, the grantee documented significant increase in usage since the start of a recent conflict, with over 1.3 million users utilizing the technology to access information in a given day.[29] This tool is currently the "number two overall app downloaded," second only to money transfer apps in one of its target countries.[30] Similarly, usage in another country soared during recent protests. Technology Project A's tool provided access to approximately 1.2 million users over a span of two days, when other technologies were blocked.[31]

The success of some sampled grants was not meaningfully captured by tracking the number of average monthly users, but by other project-relevant metrics.

For example, while Technology Project C supported 16 novel open-source privacy and security tools, they did not directly host the tools under their project. This made user-based metrics infeasible. However, the development and integration of user-to-developer feedback loops ultimately allowed these 16 technologies to incorporate feedback from more than 480 at-risk end-users after partnering with 59 digital security trainers from 26 countries.[32] Similarly, Technology Project D did not report average monthly users but tracked cumulative totals. At the end of 2019, it was being used to protect 405 civil society websites.[33] Taking readership of those websites into account, Technology Project D has served approximately 70 to 80 million unique readers each year, constituting about 2 percent of the global population of people connected to the Internet.[34] Of particular note was the success of their system in protecting those CSO websites.

Indicator 1.1-3. Number of average monthly contributions to the DRL IF supported tools. This indicator measures the number of average monthly contributions made by individuals outside the paid grantee to support the development or sustainment of the tool. It is intended to track the level of community support and participation in the tool, which should promote tool sustainability.[35] It is unclear to what extent, if any, DRL/GP supported tools received contributions from external users. Although grantees solicited feedback from end users (discussed above), sampled grants did not actively seek out nor appear to receive contributions from external users. None of the sampled grants reported on this or a similar indicator.

Effectiveness Towards Pillar 1 Values

The sampled grants effectively promoted the numerous values under the technology pillar. Specific values were emphasized by interviewed stakeholders and are illustrative of the grantees' broader embodiment of the full set of the Technology pillar values. These include the values of transparent and open-source technology as well as user-centered design. The grants' effectiveness that reflects these core values is discussed below.

Being open-source and transparent in the usage of data are key aspects of the sampled grants that developed technology tools.

Grantees value the open-source nature of their technologies as a foundational aspect to the spirit of their work and of the communities they serve. As one grantee shared, "we have been quite proud in publishing all of our work open-source…and we still have 99.99 percent network uptime. So, it does not help attackers, knowing how we built [the open-source tool], to bring us down."[36] Relatedly, several stakeholders echoed these sentiments, perceiving open-source technology as a baseline expectation when delivering technology solutions in the Internet freedom space. One grantee highlighted the use of third-party auditing, demonstrating their embodiment of being open-source in alignment with DRL/GP's values. Third-party auditing was also cited by another grantee as an important quality check on the programming as well as a tangible way to demonstrate how technologies are open and transparent. As codes are updated and revised over the years, "we will get that same module audited again. […] and we'll make the code public."[37] Open-source tools do have limits, however. For example, open-source technology often—but does not always—mean free technology, which is the preferred solution for many end users. "Nine times out of ten we are looking to recommend free services or free tools, but that is not always possible nor is it always the best option for a threat model."[38] Furthermore, open-source tools often contain limited warranties, lack extensive technical support, and can be challenging for the end user to mobilize. This may be a reality in some contexts, but it may also reflect the need for further investment to meet those needs, emphasizing the importance of user-centered design when developing new tools—one of DRL/GP's key values, as described below.

Transparent usage data was similarly understood by stakeholders as a necessity in this work. The utmost care was taken by all of the interviewed grantees developing technology tools to keep user information secure. This approach was apparent in the operation of the technology—as one grantee shared, "we cache things and we hide the origin" to keep users secure.[39] Additionally, grantees emphasized the importance of collecting as little information about users as possible. "None of the ways we collect information requires anybody to identify themselves," even when users are initially setting up their account.[40] While still upholding user-privacy, the only concession made across the Technology Projects, was the collection of geographical information at the country-level to understand the reach and measure the success of the particular tool.

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."[41] 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. One grantee reported having "interesting conversations with a few of our technically advanced clients. They are interested in the guts of our system, how it works, what does it save, how they can leverage our system in a better way."[42] Their tool was available to organizations facing specific security threats, but organizations that wanted to take a deeper dive into the tool to adapt it to their specific needs were welcomed by the grantee. Additionally, one DRL-funded technology includes a user feedback messaging system that has been the source of extensive user feedback and diagnostic data. With approximately 35 million users, they receive on average 150 feedback messages every minute. This data is "very important for running the network" and is fed into the analytic systems that drive service improvement.[43] Technology Project C sought to connect users with developers specifically to improve tool usability; the grant documented positive results from this feedback loop, including the immediate changes made by the developer of an encrypted email service. In order to scale the concept, the grantee developed a guidebook to facilitate the feedback loop between users and developers which remains in use today.[44]

> “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 Internet Freedom Grantee

Accuracy and Relevancy of Pillar 1

Access to Benefit and Participate in the Global Internet

Taken together, anti-censorship and secure communication have been and remain essential elements to allow one to access the global Internet.

Today more than ever, online surveillance is being used to collect user data, access protected information, and track user location and behavior. The surveillance market, and the growing incentives for obtaining user information, gives more leeway to governments "than ever before to flout the rule of law, [and] monitor private communications at their own discretion…."[45] Human rights laws and technology regulations have struggled to maintain pace with the rapidly evolving online ecosystem, particularly with respect to the expansion and use of these technologies for surveillance and the protection of one's privacy through secure communications. As one grantee pointed out, the approaches and methods to sensor, track, and monitor online activities are constantly being improved "and so anti-censorship [and secure communication] technologies also have to improve."[46]

According to existing research and best practices, having the ability to access information through anti-censorship technology, however, does not guarantee one's consumption of information. In other words, as described by an independent SME, anti-censorship technology alone "does not really protect [users]."[47] Without mitigating the perceived risks in accessing or sharing information through secure communication technology—providing users with the confidence and sense of security that they need to actually take the steps to consume information—Internet users will not fully exercise their human rights.[48] Thus, while anti-censorship tools are critical to enabling access to the global Internet, as acknowledged by DRL/GP, "they are not sufficient to ensuring that people can access information free from restriction." [49] This is where secure communication comes in. Working in tandem with anti-censorship technology, secure communication ensures that privacy is protected and that surveillance is thwarted. Thus, communication is possible and protected from an authority's surveilling communication."[50]

Anti-censorship and secure communication technology work hand in hand to not only bypass the filtering schemes and blocks often put in place by governments, but to also empower and equip people to access and share information confidently and safely without fear of surveillance.[51] These types of technology can come in a variety of forms such as VPNs, traffic obfuscation technologies, mesh networks, IP tunneling, encryption, and authentication, among others.[52,53] However, these are but two critical factors within the broader and evolving context of digital repression that limits one's ability to fully exercise their human rights online and offline.

The DRL/GP anti-censorship theory of change posits that if people can access information without censorship, "that it will have a transformative effect on their personal and political situation."[54] While this can be true, SMEs suggested that these tools benefit "a much smaller group of people than most think,"[55] as anti-censorship tools have "to effectively compete in a market where people are making decisions based on a variety of factors."[56] These factors, as noted by one DRL/GP representative, require "other kinds of solutions, such as policy solutions, to be implemented because of the fundamentally evolving nature of Internet governance models and the implementation and advent of Internet controls, at the governance level, in some of these country contexts."[57] While it is evident that DRL/GP and the IF team recognize these evolving demands and needs of their target communities across the IF Strategic Framework—particularly as part of the policy and advocacy pillar—the anti-censorship and secure communication theories of change do not directly acknowledge the emerging or unknown threats to "Internet governance" which are considered by stakeholders alike to be critical "for [technology] to continue to be effective."[58] In order to ensure the use and subsequently, the effectiveness of both anti-censorship and secure communication technology, actors such as the private sector, civil society, developers, and even Internet users need to have a common understanding of shared values to shape the use of the Internet. In reflection of the respective theories of change, independent SMEs thus encouraged the exploration of expanding the existing assumptions to acknowledge how the broader and evolving context of digital repression—mainly Internet governance—may impact the success of anti-censorship and secure communication technologies.

Mitigating and preventing DDoS attacks is recognized by the broader community as one of many common and disruptive types of cyberattacks repressing one's ability to participate in the global Internet, or to "share information freely".[59]

A DDoS attack is a "malevolent attempt to make an online service unavailable to genuine customers by simply stopping or delaying the host server's service."[60] In simple terms, a DDoS attack is initiated when an attacker sends a malicious packet to a specific or targeted server, known as the victim. These packets flood victim's workstations with requests to disrupt their system and deplete their resources to the point where the server begins to slow down and, in many cases, crashes or "shuts down altogether, preventing normal use and system access."[61,62] These types of cyberattacks have historically and continue to represent "one of the most critical threats"[63] to Internet use, "stifl[ing] or muzzle[ing] voices, to knock them offline at critical periods, and/or as some sort of retribution tactic for online activities."[64] Notably, the global community experienced a substantial increase following the COVID-19 pandemic, upwards of a 22 percent increase in the frequency of DDoS attacks.[65] These attacks which represent devasting violations to freedom of expression, have also become increasingly cheap to implement over the years.[66] Thus, stakeholders alike—including independent SMEs and grantees—agree that to maintain free, open, and secure communications it is imperative to prioritize a suite of cyber-attack defense mechanisms, such as DDoS mitigation, validating DRL/GP's DDoS Mitigation theory of change.[67]

Human Rights Defenders, Civil Society and Independent Media

DRL/GP-funded technologies hold the potential to impact a much larger range of users, amplifying the impact of Pillar 1.

Notably, all interviewed independent SMEs confirmed that the Anti-Censorship, Secure Communications, and DDoS Mitigation theories of change were "valid,"[68] "solid,"[69] and "accurate."[70] However, while designing technology for a specific target audience is a critical component of mitigating the illicit use of technologies, as described in more detail below, a few SMEs expressed the view that only targeting specific populations of users—human rights defenders, civil society, and independent media—limits the potential impact of this work. Many SMEs acknowledge that the work that DRL/GP is doing within the technology sector is critical. One SME in particular noted, that "in the absence of the level of funding from the U.S. government and from DRL, [the Internet freedom community] would be in a very different place than if this work did not exist."[71] In light of this and in reflection of the Technology Pillar theories of change—largely the Secure Communication and DDoS mitigation theories of change—SMEs suggested the expansion of the target audience to also include citizens in repressive environments.

Overcoming Restrictions Online and Protecting Communications

Technology is viewed as a temporary solution to, in part, overcome restrictions online and protect one's ability to receive and transmit information.

While technology is perceived by stakeholders alike as a powerful and often reliable tool to ensure access and participation in the global Internet, particularly in a repressive context, it is not a guarantee. "There is a lot which is broken in terms of law, as well as society that cannot be fixed with technology."[72] As noted above, DRL/GP-funded technologies have proven effective to address these constraints, in part. Yet, technology cannot provide users with a silver bullet to obtain Internet freedom. The Internet freedom community has seen, time and time again, "cases where a free and open Internet does not always lead to the flourishing of democratic principles" and one's ability to exercise their human rights.[73]

As emphasized in the DRL/GP IF Strategic Framework, a cross-disciplinary approach, leveraging technology development, digital safety, policy and advocacy, and research, for example, is imperative to upholding human rights online. As one SME noted, "I think we do a disfavor to ourselves when we try to examine all of these issues with only one lens or through one pillar. And that is why they have to be much more comprehensive in terms of what the tech does, and what's the environment in which tech operates. But obviously, the governments are getting more sophisticated and smarter. And that's why the legal and regulatory environments are also pretty important."[74] Technology needs to be combined with advocacy, digital safety, and research efforts, among others, to provide a comprehensive package of support to target communities and population groups. While DRL/GP's overarching IF Strategic Framework, refer to Figure 2, does recognize and employ a comprehensive approach, the individual lines of effort and theories of change—and subsequently the actions of the grantees—do not directly articulate these dependencies.

"Authoritarian governments, and let us just say illiberal governments, are taking [a broader set of actions] to repress the rights of the users using online technologies," than we have seen in the past.[75] Authoritarian or illiberal governments "are using all the tools at their disposal" to restrict communication, enhance surveillance, and suppress freedom of expression. [76] As the ecosystem continues to evolve, technology solutions and the strategy surrounding their design and deployment should foresee monitoring and updating strategies to deal with the ever evolving list of threats. DRL/GP's prioritization of user-focused design in technology development programs is thus helpful since it brings to the front of the technology development the conditions a certain user faces and will face.

ADVANCEMENT TOWARDS IF FRAMEWORK GOAL

DRL/GP-funded tools have been essential for the Internet freedom community.

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 evident by the effective progress against the Technology pillar indicators and values, described above, the sampled grants were successful in pushing towards this goal. The theories of change and underlying assumption which inform the DRL/GP Technology Development Pillar as validated by independent SMEs, moreover, accurately reflect the historical and evolving nuances of technology development within the Internet freedom ecosystem.

> This is really an area where DRL is providing a central support to [technology] products and services, 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 this program didn't exist.
>
> Independent SME

Furthermore, as echoed by another independent SME, DRL/GP-funded "tools have been largely successful in what they are trying to achieve. You can look at user statistics to easily validate how much [the tools have] grown. Usage not only demonstrates the kind of efficacy of the tools from a technical perspective successfully countering more sophisticated and aggressive forms [of repression], but also demonstrates the trust that users have developed in these tools over time. This speaks also to the success of DRL's overall approach, investing in the maintenance of critical tools that people are relying on a daily basis, while also investing in innovative new technologies to making sure they are staying one step ahead of new [threats and] techniques [to repress societies online]."[77]

A holistic approach to technology development that considers the context of the user at a macro and micro level, is critical in dealing with the ever-evolving quantity and quality of threats to promote resiliency.

Supporting a plurality of tools is an integral part of promoting the DRL/GP Technology Pillar's goal. Advances in censorship, filtering, and other malicious technology can suddenly eliminate the availability or full functionality of a specific tool in a specific location. Rapid adoption or widespread use of a specific technology can also lead to tailored blocking that specifically targets the tactics used by those tools. Funding a plurality of tools helps to mitigate against those risks in the "cat and mouse game of censorship and anti-censorship."[78] 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.

In addition, when considering the effectiveness and resiliency of technology from the end-user's perspective, it is also imperative to acknowledge that some societies still limit the ability of a user to even access those tools in the first place. An interesting point raised by one grantee in particular, and echoed by several SMEs, was the relationship between privacy for tech and access to the device itself. Donors and developers need to be mindful of the potential constraints one can encounter regarding access to a device that a particular technology is intended to be deployed on, particularly in complex or repressive environments. For example, "in more patriarchal societies, sometimes women don't have access to a private device. Similarly, when working with parents or caregivers, [it is important to be mindful that these users] might be sharing their device with others in the household."[79] Often times, even if these marginalized populations have access to devices, they may not have agency to make the decision about what type of software is installed on that device, or what types of tools they are able to use. Furthermore, downloading or installing these types of tools on a device may raise flags or result in unintended harm to the end user.

SAFEGUARDS

Background

At the core of the IF Portfolio lies the aim "to protect the open, interoperable, secure, and reliable Internet by promoting fundamental freedoms, human rights, and the free flow of information online through integrated support to civil society for technology, digital safety, policy and advocacy, and applied research programs."[80] While promoting these values and capabilities, the IF Portfolio's Technology Development pillar supports 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."[81] And while these tools 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.

This situation presents the possible trade-offs of any technology—as technology is neutral in theory, it can be used for good or bad by those who develop it, control it, access it, and/or use it. Specifically, while helping to promote and provide "safe, reliable, and anonymous Internet access to people who would otherwise be censored, filtered, or punished for communicating electronically,"[82] anti-censorship and privacy protecting technology could also help certain actors "to conceal or commit illegal activity"[83] and even present a threat "to other aspects of … national security."[84] "Respect for individuals' autonomy, anonymous speech, and the right to free association must be balanced against legitimate concerns like law enforcement."[85]

The exercise of Internet freedoms requires anonymity and privacy to protect human rights activists and defenders of democratic values, minorities, and vulnerable groups across the world. Anonymity is essential to protect these users from "political or economic retribution, harassment, or even threats to their lives."[86] Furthermore, "the right to anonymous free speech is protected by the First Amendment"[87] and is a crucial enabler of the right of Freedom of Expression as established in Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[88] In general, the free flow of information, opinions, and data helps foster transparency, creativity, innovation, and learning, and tools and methods that support this flow generate positive economic, social, and political consequences.

At the same time, however, criminals can also use encryption and anonymity tools to conceal and enable their crimes. Society has an undeniable interest in law enforcement being able to investigate and prosecute criminals. Some level of online transparency, attribution, and traceability, among other features, could be used to increase the ease by which law enforcement are able to identify and prosecute criminals. Law enforcement and intelligence agencies who can develop the capacity required to gather, sort through, and correctly interpret the abundance of available digital information can use it to strengthen their investigations and analysis. In other words, as the privacy of online users is degraded and the security of digital communications is reduced more personal information is available for use by law enforcement, intelligence agencies, and many others. Considering these legitimate Law Enforcement interests implementing safeguards that can mitigate the risk of using such tools for illicit purposes while still preserving their ability to allow the exercise of Human Rights online is of high importance.

Establishing Safeguards

Illicit Use Mitigation Strategy

DRL/GP has successfully developed a strategy and approach to mitigate the illicit use of funded technologies in alignment with international standards and best practices.

In appropriating funds to DRL/GP, the U.S. Congress has expressed its concern for the potential use of technologies for illicit purposes, such as cyberterrorism, sexual exploitation, algorithmic discrimination, and lack of transparency, among others.[89,90] DRL/GP has acknowledged this concern by establishing an internal process, the Illicit Use Mitigation Strategy,[91] to mitigate these risks by deploying safeguards throughout the grant cycle. As summarized in Table 2 below, the Illicit Use Mitigation Strategy includes three core or foundational safeguards that are implemented throughout the grant cycle and the development of technologies.

Table 2. DRL/GP's Illicit Use Mitigation Strategy[92]

Safeguards
1) Application of a human rights framework to Internet freedom programming, which includes software development consistent with the human rights use case, and the development of human rights and technology community standards
2) Application of proposal and project review controls, to assess the risk of illicit use throughout the proposal review and project implementation cycle
3) Evaluation, on a periodic basis of illicit use

The first safeguard consists of the application of a human rights framework to Internet freedom programming. The human rights framework entails having companies and tech developers "commit to designing tools, technologies, and services to respect human rights by default, rather than permit abuse or exploitation as part of their business model."[93] As DRL/GP described, the IF Portfolio human rights framework is composed of three core principles: (1) the human rights use case, (2) a specific target audience, and (3) a user-centered design. When requesting, evaluating, and selecting proposals, DRL/GP focuses exclusively on funding technologies that are developed and/or designed to benefit human rights defenders and/or members of marginalized and vulnerable population groups. The second safeguard consists of an internal and individual risk assessment of each proposed technology or tool by DRL/GP expert staff. Finally, the third safeguard—periodic evaluations, provides DRL/GP with an unbiased, independent, third-party assessment to measure the effectiveness of the IF Portfolio and its safeguards in mitigating illicit use, among other research topics.

Taken together, the commitment to a human rights-based approach, in conjunction with the application of individual risk assessments and periodic evaluations, encompasses actions to "prevent filtering companies from designing their technology with features that enable large-scale, indiscriminate, or inherently disproportionate censorship capabilities" and having "algorithms incorporated into the design of communications and storage platforms" that "could account for human rights considerations in addition to business objectives."[94] Ultimately, this suggests that tools that are designed and developed within a human rights-based approach, with the goal to protect and promote human rights, should have less potential to be used for illicit purposes than comparable technologies designed without a human rights-based approach.

The IF Portfolio is built on a foundation of universally recognized principles that mitigate the illicit use of technologies.

A core principle is the development of such technologies within a human-rights framework, which is foundational to mitigate the illicit use of technology designed, for instance, to circumvent censorship to publish, post, and share information or to provide access to information online and offer secure communications while protecting anonymity. The application of a human rights framework, the first safeguard embedded within DRL/GP's Illicit Use Mitigation Strategy, "require[s] software development [that is] consistent with the human rights use case, and the development of human rights and technology community standards."[95]

This emphasis fundamentally grounds "the development of the technology for human rights rather than for other purposes."[96] Ultimately, this suggests that tools developed within a human rights framework, with the goal to protect and promote human rights, should be less useful and effective at serving illicit purposes than comparable technologies designed without. This emphasis thus distorts the "neutrality" of a technology towards the side of the "good," implicating its design and application. For example, "mainstream services like WhatsApp and iMessage" have historically, more commonly been used by criminals than their comparable technologies "because they are cheap, easy to access and allow [any individual] to communicate with a wide audience" with ease for their illicit products and activities.[97]

Furthermore, as explained by DRL/GP, this safeguard is also related to the need to "look for very specific human rights applications" that need to have user-centered design that targets—via its technical and linguistical design and also outreach and engagement strategies—a specific audience, most often "human rights defenders for independent media work, civil society and marginalized populations"[98] —that is "people who are suffering under repression of human rights, women, people with disabilities, racial and ethnic minorities, religious minorities, and lesbian, gay, bisexual, and transgender (LGBT) people."[99] Thus, these three complementary principles show clear alignment with the universally recognized "human rights by design" principle, in which "tools, technologies, and services" are committed "to respect human rights by default, rather than permit abuse or exploitation as part of their business model."[100]

> 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

Promoting human rights as part of technology design reduces the risk of these tools being used for illicit purposes.

Current research[101] suggests that criminal actors have different needs, hence different use cases than human rights defenders meaning that the technology used by these two audiences tend to be fundamentally different. Therefore, selecting technology based on its specific human rights application and developing the technology for a specific target audience, as expressed in the safeguards applied by DRL/GP, has proven, to date, to be an effective choice to reduce the likelihood of technologies being used for illicit purposes. However, while proven to drastically reduce the risk of illicit activity, the human rights use case,—like other safeguards,—cannot fully prevent individuals from deploying any technology for illicit activities. Specifically, independent SMEs acknowledged two subtle vulnerabilities or risks that may present when employing the human rights use case:

- First, the human rights use case is grounded in Human Rights which has its "own set of ambiguities," just as any set of rights, rules, or norms, meaning that it can also present flaws. Nonetheless, Human Rights are "known and less changeable" than other sets of rules and principles, making it the safest reference for selecting technologies to fund and foster.

- The second vulnerability is the potential risk of exposing the population to a technology it wants to actually support. Rather than "hid[ing]" or protecting these users among a larger population group, technologies that are designed primarily or exclusively for human rights defenders can place a target on their back, as is the case of some messaging platforms. "(…) making sure you have a specific target audience [can] actually [be] counterproductive for people's privacy, sometimes insecurity. Using a bespoke special tool might signal to someone that you are actually engaged in freedom protecting activities and target you." [102]

While these vulnerabilities may not impact the efforts to mitigate illicit use, they are vulnerabilities that the mitigation itself creates for the technology and their intended beneficiaries.

DRL/GP conducts internal risk assessments as part of the technology selection process to reduce the probability that a funded technology will be used for illicit purposes.

After analyzing the alignment of the proposed technology with the human rights framework, DRL/GP moves onto the second safeguard during the procurement process: the application of review controls to the proposal presented. DRL/GP has developed an internal risk assessment process to review and assess the risk of illicit use of technologies funded throughout the proposal review and, also, during the program implementation cycle. Specifically, during the procurement process, DRL/GP assesses and scores each application against a myriad of topics regarding risks consolidated into an Internal Risk Assessment Tool template. This assessment is done independently of the applicants and subsequently, the awarded grantees, so that an impartial assessment of potential risks is reached. As a result of the independent nature of the donor-led assessments, applicants, and the awarded grantees, most often are not involved or informed about the process or results. "(…) We [DRL/GP] are assessing independently; they [the applicants] never see the risk assessment. They [the applicants] never see that evaluation."[103] If however, DRL/GP identifies or perceives a potential issue with a proposed technology during the application stage—particularly with a promising, high value technology, DRL/GP establishes "conditions" and/or provides "recommendations" to the applicants, prompting the revision and resubmission of the proposal to mitigate illicit use.

Based on a review of the Internal Risk Assessment Tool template itself, it is unclear to the evaluation team how and what steps are taken to effectively assess and document potential risks of illicit use for any given technology. The Internal Risk Assessment Tool template itself does not articulate the kind of content that informs the assessment—for example if the documentation used to assess risk is included as part of the grant application, if DRL/GP consults and/or validates the results with independent SMEs, or if this information is obtained exclusively from DRL/GP's internal experts. In addition, the template does not include a pre-established set of rubrics or a scoring system to ensure consistency in its use or to compare results across proposals. The evaluation team was not able to access historical records to demonstrate this process in detail and, subsequently, the results of prior proposal assessments. Thus, the evaluation team was unable to fully measure the effectiveness of the assessment tool and its criteria in determining the potential for illicit use.

DRL/GP consistently and routinely seeks to assess the implementation of safeguards to mitigate illicit use.

DRL/GP annually reviews the Internal Risk Assessments for awarded grants first made during the procurement phase to guarantee that the funded technologies are still being developed in alignment with the human rights use case. "What we do is we assess whether or not the technology is correct, effectively and accurately as predicted, addressing the human rights use case."[104] While the evaluation team was able to review the overarching GOR Risk Assessment and Monitoring Plan and received detailed information from DRL/GP on the annual reviews of these assessments, the evaluation team did not have access to the completed annual assessments. Thus, the evaluation team was not able to fully assess and validate how the reviews were carried out, or what sort of sources are used to inform the assessment.

In addition to the annual Internal Risks Assessments, DRL/GP consistently and routinely funds independent, third-party evaluations of the Internet Freedom Portfolio which, among other things, has historically included an assessment on the effectiveness of its established safeguards. Both of these efforts, or safeguards, are anchored in the prior safeguards and principles identified.

DRL/GP does not monitor the frequency at which funded technologies are used for illicit purposes—and, generally, neither do grantees.
"We do not assess, specifically, how many illicit uses have happened as a result of support for one particular technology or another."[105] This is not part of the annual risk assessment nor is it required of grantees to monitor and report. DRL/GP is "not going out there and conducting research on whether or not the technology is being used by terrorist actors or other illicit actors." Therefore, DRL's internal efforts to monitor and evaluate the effectiveness of its safeguards tend to be more focused on the mitigating future occurrences of illicit use, than on understanding if and how current DRL/GP-funded technologies have been used for illicit purposes. This, however, is in large part due to the fact that investigating or monitoring illicit uses of tools cannot be done without breaking user's privacy—which does not align with DRL's privacy-by-design principle.

> "… privacy by design, is a technological feature of much of our programming. And so, privacy by design means that we emphasize and encourage minimal tracking of users by technology platforms that we support. The technology programs may have the ability to collect a certain amount of information about the number of users that they have, but they don't collect as much as they could, because doing so would imperil the user. We neither request nor encourage them to, nor do we want that information communicated to a US government official for the safety of that individual user."
>
> DRL/GP Representative

Understanding the Potential Risks of Internet Freedom Technology

The Potential of Anti-Censorship Technology for Illicit Use

According to the grantees, the two selected projects of the Anti-Censorship Line of Effort are focused on providing access to content. One of them works as a browser-based VPN tool and the other provides access to media apps through secure peer-to-peer distribution directly embedded into the apps. The first and most relevant risk identified as part of DRL/GP's work related to promoting anti-censorship, and thus supporting the potential access to information and context, was the obvious risk that the technology could be deployed as an **anonymity tool to access illegal content for an illicit activity**. Grantees and SMEs, however, both emphasized that these types of technology are not designed to ease or support illicit purposes—rather they are intended to provide access to information. According to the grantees and due to other human rights-based safeguards, the users that will potentially use anti-censorship technology to potentially access "illicit content"—which cannot be blocked because the use of the technology, is not monitored to preserve user privacy—a fundamental right also aligned with the human rights use case.[106] "If someone accesses 'illicit' information through this app [or technology], we will have no way of knowing." [107]

SMEs expounded on this, noting that if DRL/GP were to monitor users' activity across its funded technologies to detect illicit use, this would severely contradict the purposes of the program and would be counterintuitive for the purposes of promoting human rights online. To ensure the protection of human rights, one of the DRL/GP grantees noted that, "[The technology] is encrypted, in every way, developed to make it impossible to anyone including us to know what's passing through the system."[108] Another grantee highlighted that, "the most personally identifiable thing is someone's IP address. [While we record the geolocation of users (i.e., country),] because DRL wants to know, that's the only concession we make. From there, [everything is] shredded and diced up and all the cryptographic ways you can destroy that IP address. So, it does not exist anymore and it is tossed away. Now, from that point on, there's no more personally identifiable information related to IP address."[109]

The second risk, given that DRL/GP-funded technologies are open source, is the risk that any given application or technology could be **copied or reproduced—in totality or in part—generating new or derivative versions** of the application. In this hypothetical scenario, the creators of the "new or derivative version," if portrayed, for example, as being the original application but in reality is a "fake," would be seeking "data" from users or would aim to resell it for profit. Another hypothesis is that the application or technology could be easily copied, thus reducing the development costs for individuals seeking to replicate the technology potentially for "illicit use." While this scenario is possible, it is highly unlikely due to a series of characteristics of the types of DRL/GP-funded technologies. For instance, as one of DRL/GP's grantees explained, "our application or our network is relatively slow, compared to using a regular VPN… I would use a [regular] VPN, or Tor over VPN, or a browser rather than using a site phone." [110]

The Potential of Secure Communications Technology for Illicit Use

DRL/GP has funded technologies to provide users with secure communication technology and tools. Specifically, the grant assessed as part of this evaluation built a decentralized content distribution network to permit content publishers and their users to access and deploy the system for the purposes of defeating censorship. The main risk of illicit use acknowledged by the respective grantee was the **potential use of the methodology to inform another technology for illicit purposes**. The likelihood of this scenario was recognized by both SMEs and the grantees as a "stretch of the imagination" as it is quite unlikely. "I would imagine it being like, someone could use the methodologies in terms of gathering feedback for nefarious activities, or for a tool that is designed for them for nefarious activities. But I think it would be a bit of a stretch in this case. We're generally having to convince people who are doing things for good and are committed to good to care about these things." [111] However, while the grantee deemed this risk as low, the grantee acknowledged that it was possible and thus identified relevant safeguards to mitigate the risk. The grantee went on to further acknowledge, that while the tool which they developed had a low risk of being used for illicit purposes, "tools that [utilized their technology for secure communications], could certainly be used for illicit activities. And I know that that's an ongoing conversation in the community about ethics and kind of what that means."[112]

Building upon the human rights framework established during the procurement phase, the technology focuses on promoting usability of security and circumvention tools designed for "human rights activists, persons with disabilities, and at-risk groups[113] operating in restrictive, Internet-hostile environments."[114] With this clear objective, the specific audience targeted by the project is already noticeable. Besides, the project feeds off an already established network of partners from the respective grantee's previous projects. Furthermore, another core objective of the technology is promoting usability in security tools, which means enhancing and prioritizing a user-centered design that increases the adoption of security tools. However, this concern, as raised by SMEs in selecting a target audience, which can increase their vulnerability as described above in relation to anti-censorship technology, also holds true. According to SMEs, "you shouldn't design a tool, so that it can only be used by your target audience, unless you're really very confident that that's not going to be identifiable by technical or non-technical means in a way that can put them at risk." [115]

The Potential of DDOS Mitigation Technology for Illicit Use

The selected DDoS mitigation project offers secure hosting, encrypted connections, and advanced mitigation options among other features to protect websites from DDoS attacks. The goal is to make DDoS attacks less effective and "peel away at attackers' impunity by enabling attribution."[116] The primary risks identified by the respective grantee and SMEs were the risk of employing the tool to **protect illicit content** from attack, instead of protecting content aligned with the promotion of human rights, as well as having the technology's **code copied** for this specific end. Experts also raised the concern about how the tool enables **attribution to avoid violating privacy**. "A lot of DDoS mitigation tools do include trying to identify who the attacker is…, if that's the case, then there might be some privacy-violating uses…. It depends on how it's enabling attribution. If it's enabling attribution in a very narrow context about the actual DDoS attack, who is the person, who is doing something that qualifies as a DDoS attack, that would be okay. But a lot of these things use general tools to try to figure out who the person is. And I think that's very dangerous if it gets misused."[117]

Similarly, to secure communication, the DDoS mitigation grantee also understands that the identified risks of potential illicit use requires a "stretch of the imagination" due to their specific reach in that tools tend to focus on a niche audience and selected organizations that mirror the human rights use case. As stated by the grantee: "(…) these are defensive technologies by design. So, the only thing they can do is absorb traffic and differentiate between good traffic and bad traffic. In our use case, illicit use may come from protecting a malicious client and allowing that client to be online. But since we're selecting our clients, that doesn't happen, hopefully. I don't think it's very easy to get through our eligibility process by putting up a fake website." [118] Specialists also acknowledge that the particular design of the selected technologies along with their approach targeting an audience can balance the benefits of the lines of effort and minor risks of illicit use. Nonetheless, they acknowledge that there is always some illicit use risk, reiterating the perspective that there is only so much that can be done to mitigate them but never avoid them altogether.

Success of DRL/GP Established Safeguards

From the onset, DRL/GP successfully laid a solid foundation to prevent risks of illicit use of IF-funded technologies.

It is a shared understanding among stakeholders that the safeguards adopted by DRL/GP—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 of DRL/GP-funded 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. In addition, according to grantees and leading research as summarized in Annex 4, Literature Review,[119] criminals are more likely to develop their tools for their crimes instead of taking advantage of existing tools, especially the ones with a clear human rights use case that specifically target a unique audience.

In addition to mitigating illicit use across the respective lines of effort, the established safeguards support the promotion of the broader IF goals and values.

The grants assessed as part of this evaluation developed and offered technologies that are committed to **user's privacy and the promotion of access to information and content**. Thus, the technologies developed and supported by DRL/GP are fundamentally connected to the **human rights use case.** Enabling privacy of defenders and vulnerable populations is an essential enabling right for access to content, especially in censored environments, thus fulfilling Articles 12 and 19 of the Universal Declaration of Human Rights. As one grantee noted: "(…) the Declaration of Human Rights says everybody gets equal access to information, electronic information, regardless of where they are on the world that is considered a human… So, in doing that, and providing that right to people is morally, and practically, important."[120] Second, and perhaps more relevant to mitigating illicit use, grantees have committed to developing technologies based on a *user-centered design* to promote usability by the targeted communities. Specifically, one of the two anti-censorship technologies has been made available in over 40 languages and developed in such a way that the users "just have to push a button" and "off you go."[121] In comparison, the other technology has been coded in such a way that it does not “require any extra steps, additional downloads, or permissions.”[122] Finally, while these technologies are not restricted to a specific type of population, they are designed with the intention to be most *beneficial to repressed populations* under censorship that restricts some level of internet access. For instance, it is clear to one of the grantees how fast the number of users in a particular country increases when the population is facing severe internet blockages. “…the unfortunate side of that is we reflect the bad shape of blocking and censorship in the world to a certain degree…. from our perspective, we look at it as our ability to deliver across any environmental moment, no matter how harsh. And harsher ones, we tend to do better, respectively than the other ones.”[123]

However, an opportunity exists to enhance and further the success of DRL/GP-funded technologies by improving existing safeguards and integrating new safeguards to mitigate illicit use.

Although DRL/GP has established a clear definition of illicit use—as summarized on page viii of this report,[124] DRL/GP grantees do not have a clear understanding of illicit use. Relatedly, grantees do not have a shared understanding of the concept of safeguards. Without providing a definition, or an exemplification, of what DRL/GP refers to by “illicit use” in the specific context in which concerns exist, grantees have found, and are likely to continue to find, it difficult to assess potential risks of a given technology for illicit activity.

The Internal Risk Assessments conducted by DRL/GP during the procurement process, as well as part of annual grant reviews, face similar issues. DRL/GP does the risk assessments independently from applicants and selected grantees. The decision to not include grantees in the risk assessment process is valid to limit potential biases during the procurement process as well as to not put an undue emphasis on grantees for the risk and mitigation strategies. At the same time, however, following grant award, grantee engagement could be crucial. Sensitizing grantees upon award of the DRL/GP overarching Illicit Use Mitigation Strategy and approach to safeguards, would address this challenge. This approach would increase awareness among grantees on the potential risks within their respective technologies, empower them to actively contribute to mitigation efforts—being mindful of DRL/GP’s Internet freedom values, especially privacy, and prepare them for future assessments and evaluations. Furthermore, while DRL/GP noted that these internal assessments are grounded in policy,[125] collaboration with respected SMEs and thought leaders would further validate and strengthen DRL/GP’s approach to mitigating illicit use.

The evaluation team’s assessment of safeguards was limited, in part, by the availability of completed documentation related to the internal risk assessment process. Outside of discussions with the DRL/GP team, the evaluation team found it quite hard to identify specific documents outlining the step-by-step process of mitigating illicit use. This information is crucial in many aspects. Not only it is essential to inform independent “evaluations, on a periodic basis, of illicit misuse mitigation strategy, by means of external reports,”[126] but it also provides resources for the DRL/GP to be protective to demonstrate the impacts of its supported technologies as well as to validate the effectiveness of its application of safeguards.

While opportunities for improvement in DRL/GP’s efforts to monitor and assess illicit use exist, no major illicit uses of DRL/GP-funded technologies were found or disclosed within the evaluated grants.

DRL’s activity towards monitoring safeguards implemented by its grantees aims to fulfill the funding’s requirements while also protecting the objectives and principles under which each project operates—for example, human rights use case and privacy by design. DRL/GP protects both the tool and its users in that sense. This suggests that the current safeguards effectively balance both the risks and benefits to meet the objectives, goals, and values of the Strategic Framework while mitigating illicit use. Despite the opportunities for improvement as stated above, the evaluation concluded that the illicit use mitigation strategy and the safeguards put in place have, to date, effectively mitigated illicit use, with no major illicit use cases being found within the selected grantees.

PILLAR 2 DIGITAL SAFETY

Pillar 2, Digital Safety, is grounded on the assumption that training and capacity building for civil society and activists would mitigate the impacts of potential attacks and improve their understanding about digital security. The availability and reliability of emergency resources and support would also increase the likelihood that activists will continue their work and be able to withstand threats and attacks in the future. Specifically, the Digital Safety Pillar aims to "to combat violence against bloggers and other users; and to enhance digital security training and capacity building for democracy activists."[127]

THEORIES OF CHANGE AND UNDERLYING ASSUMPTIONS

The Digital Safety Pillar is comprised of three lines of effort: (1) Digital Security Capacity-Building, (2) Emergency Support, and (3) Public Awareness-Raising and Education. All three digital safety lines of effort were included as part of the evaluation. To assess the effectiveness (EQ 1) and relevancy (EQ 2) of DRL/GP's efforts related to these lines of effort, it is imperative to first understand the perceived pathway of change or theory of change describing how and why a specific or set of interventions are believed to contribute to the desired goal or end result. In addition, it is likewise just as important to understand the underlying assumptions within a given theory of change. Underlying assumptions provide a clear picture of the conditions or resources required for change to occur. Please refer to Annex 5 for DRL/GP's Digital Safety Theories of Change and identified underlying assumptions.

EFFECTIVENESS OF PILLAR 2

Effectiveness Towards IF Framework Indicators

To measure the results of its three lines of effort, the Digital Safety pillar contains indicators grouped into two areas: the emergency support and impact mitigation (program area 2.1) and digital safety assistance (program area 2.2). The DRL/GP-funded grants were highly successful in delivering emergency support and digital safety assistance to numerous diverse stakeholders, although there were some challenges translating output level success (delivering assistance to organizations) to outcome level success (organizations making changes to strengthen their security).

Regarding the number and type of actors who received emergency support, the IF-funded grants supported a diverse array of stakeholders, guaranteeing reach and diverse coverage. Program Area 2.1. included indicators on the number of requests for emergency support received and the number of actors (i.e., human rights defenders and CSOs) who received support, as well as the percentage of recipients who perceived their incidents to be resolved. Digital Safety Project C delivered emergency response resources in the form of 180 sub-grants to provide emergency support through a series of lenses. From the 180, 53 were substantiated on freedom of expression emergencies, 32 on women's rights, 29 on LGBTI+ issues, 29 on political activism or civil rights, and 11 on land, environment, or indigenous rights.[128] Digital Safety Project A delivered emergency support to 234 CSOs, far exceeding the initial target of 15.[129]

In addition to the quantity of emergency support provided, the grants were highly successful in delivering targeted support that resolved the incidents at hand.
Ninety-eight percent of surveyed sub-grantees under Digital Safety Project C agreed that the support they received directly dealt with to the threat(s) they faced, and 79 percent agreed they felt safer following the intervention.[130] Of note was that organizations receiving emergency support sub-grants under Digital Safety Project C could use those funds to cover a wide range of expenses that other emergency funds often exclude. This included "expenses like digital subscriptions, software, devices, mobile devices, laptops, those kinds of components, which [is what] victims of digital attacks or activists [who] experience digital emergency… need the most."[131] Digital Safety Project C sub-grants could also contribute to cover legal fees for journalists, for example, who were being prosecuted.

Digital Safety Project A similarly delivered targeted and tailored emergency support by offering emergencies services via local technology labs that received sub-grants. Digital Safety Project A developed regional threat labs that could deliver "direct incidence response" to local CSOs, providing "bespoke and high tier" technical expertise contextualized to the region and within the recipient organization's own time zone.[132] The threat labs also provided important threat warnings to their broader communities. The number of organizations that benefitted from these threat warnings is not known, but the threat labs would disseminate key indicators and characteristics of a consistent threat actor to "put other people in the community who have similar characteristics on alert."[133]

Digital Safety Project A experienced some challenges in identifying appropriate organizations that could serve as threat labs in all the selected regions, particularly in the Middle East and North Africa (MENA), and not all threat labs had the sophistication to deliver the same level of services.[134] However, the threat labs in Eastern Europe were extremely well-equipped and provided important emergency support. One such success story comes from a benefitting organization under Digital Safety Project A. The benefitting organization analyzed a host government's COVID tracker app's code and discovered it acted as spyware—pushing the government to recall the app and develop a safer one (refer to box). The organization worked collaboratively with the government and helped to ensure the national COVID tracker app was privacy-oriented.

Similar to emergency support, activities contributing to the digital safety assistance engaged numerous and diverse stakeholders.
Program Area 2.2.—digital safety assistance indicators included the number of individuals and groups trained on digital safety techniques, the percentage of trainees with improved digital safety practices, and the number of educational resources and engagement opportunities created by the grant. These indicators all emphasize building the capacity of individuals and groups to understand and implement digital safety techniques. As one interviewed stakeholder shared, the first step is to help CSOs identify when there is a security issue, then help them learn how to respond to it. "If you don't know you're being attacked in the first place, if you can't detect that something has happened," then you cannot act. Once that baseline knowledge was developed, "we could then pivot into building the capacity of civil society [to] analyze these types of artifacts."[135]

Digital Safety Project B delivered training modules directly to beneficiaries. Digital Safety Project B trained 57 individuals (the target was 10) with the goal of "expanding the number of safe tag auditors."[136] The grant additionally built out technical training content and modules to further support capacity development. One benefitting organization then went on to train 50 individuals (the target was 34)—including 27 men, 21 women, and 2 non-binary individuals.[137] The grant set a target for beneficiaries to increase their digital security skills by 25 percent and, based on pre- and post-testing, skills increased by 46 percent with all beneficiaries demonstrating improvement.[138]

Extending beyond traditional trainings, DRL/GP-funded grantees facilitated annual events gathering actors across the Internet freedom space to further grow and educate the community.
Under line of effort 8 Public Awareness Raising and Education, for example, the Digital Safety Project E developed and hosted an annual conference that gathered Internet freedom and digital security actors "to connect, expose people to the ideas, community, and solidarity and most importantly, the things that we all work on, which are technology, advocacy, Internet freedom and research policy."[139] Digital Safety Project E garnered 5,305 registrations over the course of the project and registrations more than doubled between the first and final years of the grant.[140] The grantee also focused on increasing participant diversity. By 2018, the conference achieved gender parity among registered participants and, thanks to a diversity and inclusion fund support by diverse donors including DRL, "over 50 percent of attendees [were] from the global south by the end" of the grant period.[141]

> "By 2018, Digital Safety Project E achieved gender parity among registered participants and, thanks to a diversity and inclusion fund support by diverse donors including DRL, "over 50 percent of attendees [were] from the global south by the end" of the grant period."
>
> DRL/GP Internet Freedom Grantee

Digital Safety Projects A and B reported conducting organizational digital security audits.
Digital security audits are useful tools to identify issues or risks to an organization's digital safety. These audits are designed to place useful information into the hands of an organization to empower that organization to make informed decisions on how to enhance or strengthen its digital safety. Exceeding their targets, under Digital Safety Project B there were 30 audits (exceeding the target of 20) and under Digital Safety Project A there were 13 (exceeding the target of 5).[142]

While the purpose of an audit is to create organizational awareness, the intended impact of an audit is that an organization will undertake the arduous process of organizational transformation, allocating the necessary resources, capacity, and commitment required, to substantially improve their security against repressive threats. Despite exceeding their targets; however, the limited available evidence suggests that little to no changes in organizational digital security practices were made in response to those audits. For example, the Digital Safety Project B reported that none of the audited organizations who participated in their midterm evaluation call reported substantially improved digital security practices during the project period (the target was 60 percent).[143]

The audits provided roadmaps for organizations to strengthen their security practices.
In contrast to the strategy employed by Digital Safety Project A, the audit process under Digital Safety Project B included "not only a full report coming out of that audit, but also a full list of specific and very concrete recommendations that the civil society organizations or media outlets can implement."[144] Despite the robustness of the audit framework, the Digital Safety Project B "[could not] ensure that the CSOs will address all the audit recommendations," and as reported by the Digital Safety Project B, none of the audited organizations did significantly improve their digital security during the project period.[145] However, these interventions were helpful as they often included recommendations on the adoption of specific new software or devices. As one interviewee explained, "people [burn] out very quickly. The only way you scale security is with automation, and products are the things that help you automate that security."[146] To this end, while the Digital Safety Project A grant was unsuccessful in its attempts to build relationships between civil society and private sector cybersecurity firms, its interventions were "highly successful in securing free device endpoint protection and pro bono licenses for cybersecurity tools, distributing over $260,000 worth of licenses to support digital security for journalists and civil society organizations."[147]

Effectiveness Towards Pillar 2 Values

The sampled grants successfully reflect key aspects of the Digital Security Pillar values, specifically in their use of accessible local solutions that promote holistic security. The grants' effectiveness reflected in these core values is discussed below.

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.

Digital Safety Projects A and B—trained regional auditors within an audit framework and established regional threat labs, respectively, to deliver timely, contextualized support to local organizations. The audit framework is capable of being adapted to diverse scenarios and contexts. "The key element, however, to this adaptability and multi-functionality lies in ensuring that those who administer it are familiar with both the framework, but also with the environment in which the target organization operates."[148] Through its training of auditors around the world, Digital Safety Project B established localized resources capable of addressing local security needs. Similarly, the majority of the threat labs under the Digital Safety Project A were optimally positioned—geographically and regarding their technical capability—to analyze threats and "share information back to the community regarding attack trends, emerging threats, and countermeasures."[149] One example of the threat lab's success in delivering timely localized responses is seen in their data-driven evolution of services. The grantee and the threat lab had initially anticipated "a lot of sophisticated malware attacks. But once we analyzed all of the threats that were coming in, we found that phishing is a huge, huge problem."[150] The activities and resources of the threat lab were retooled in response to local need.

Similarly, Digital Safety Project C promoted regionalized networks to disperse expertise and facilitate connections and exchange of expertise between local stakeholders. Digital Safety Project C regionalized the rapid responder networks to connect actors across the globe. Further, they developed a digital integrity community of regional fellows in addition to global fellows to support and motivate local security leaders. During the course of the grant period and the years since, their team "has grown from four people in Europe to now 45 people in over 20 countries […] and most of them are providing support to organizations where they're actually based."[151]

Additional values under the digital security pillar emphasize data literacy, education, and making information and tools accessible. Digital Safety Project E, for example, emphasized education within the conference agenda and facilitated numerous self-organized sessions where attendees could direct discussions to areas of interest as defined by the community.[152] Digital Safety Project F added new content "on topics such as Workplace Raids, Online Abuse, Whistle-blowers, Online Privacy, Censorship and Terrorism;" Digital Safety Project F implementing further translated the app into Arabic, French, Farsi, Chinese (traditional),and Russian to enhance accessibility.[153]

Most grants emphasized digital security, but some successfully wove in solutions for physical safety as well.

A final standout value under the pillar is to promote holistic security, which includes digital security as well as physical and psychosocial security. Nearly all sampled grants focused exclusively on digital security. However, Digital Safety Project F included elements to respond to physical security threats as well as digital security threats. Stakeholders recalled human rights defenders who had the Digital Safety Project F technology on their phone "because they've been doing digital security training with us;" but upon their kidnapping, these individuals utilized the tools in the app designed specifically for physical security incidents. "They had [the technology] on the phone for one reason, they ended up using it for another reason completely separately. But this is why we built it the way we did."[154] The grantee designed the Digital Safety Project F app to provide information and resources for a holistic range of security threats, and these diverse resources were actively used by human rights defenders.

ACCURACY AND RELEVANCY OF PILLAR 2

Empowering Civil Society and Marginalized Populations to Protect Themselves

Tailored resources and targeted capacity building efforts are critical to empowering civil society and marginalized populations.

Information on digital safety and ways to prevent and respond to digital attacks is widely available across the Internet, in "formats ranging from mobile apps, video, and animation through to plain text."[155] However, while readily available, information can easily misguide users due to contradictory recommendations among sources and target audiences with varying levels of capacity and baseline understandings. Furthermore, resources are often available in a limited number of languages reducing the accessibility of information.[156] To effectively support civil society and particularly marginalized populations against potential digital attacks as well as to ensure their resiliency when facing a digital threat, it is imperative that resources and capacity building efforts are designed with the target user in mind. "The access [to resources] has to be tailored… because of the different populations, because the public is so broad."[157] Importantly, as DRL/GP grantees pointed out, it isn't just about tailoring or creating individualized resources—it is also imperative that resources are localized. "Any localized educational resource will be more effective if it is an individual resource. And any individual resource absolutely has to be localized." [158]

A wholistic approach to digital security—combining tailored resources and targeted capacity building efforts with awareness raising—is required to effectively empower civil society and marginalized populations working in adverse circumstances to ensure resiliency to digital threats.

Despite an increase in the availability of technology and resources designed to help individuals protect their personal information online and respond to imminent threats, there is a growing understanding that technology alone cannot protect people's digital security. Ultimately, as online users are the ones who choose to, and need to know how to, adhere to security procedures, if users themselves do not properly deploy and utilize the available technologies, their digital safety is still at risk. As the race between technology that protects and technology that harms is constantly evolving, it is essential that users understand the advantages, disadvantages, and limitations of these technologies and their intended use as well as the recommendations and guidelines on how to protect one's digital privacy by identifying digital threats, which are often "hard to understand or act on."[159] To address these constraints, it is widely understood by leading experts, including DRL/GP staff, that tailored resources, targeted capacity building efforts, and public awareness raising activities are effective methods to equip civil society and marginalized populations with the knowledge, skills, and behaviors to promote a safe and rights-respecting digital ecosystem for all. The impacts of these efforts are only enhanced when combined as a comprehensive package for communities to access. As DRL/GP noted, "there is not a particularly systemic way that we are approaching digital safety at the global scale, there are stakeholders at the regional level, who drastically shape the way in which digital safety responses are playing out in those specific regions" further emphasizing a tailored and localized approach to mitigating digital threats.[160]

To empower civil society and marginalized populations, digital safety resources are most effective when employed at the organizational level.

Beyond individual online users, the need for digital safety also extends to and intensifies at the organization level. For organizations, including philanthropic, civil society, media, and human rights organizations, digital security is of utmost importance as they are often the target of digital attacks, and, in some cases, physical attacks to their offices. Improving organizational level security—leveling the playing field of security across the organization in a way that is not individual-staff-dependent—supports long-term security, stability and resilience. "I actually tend to think that this is right, that this is really about organizational capacity building versus individuals. And I think that all of this is absolutely critical."[161] Thus, these organizations have different needs considering they have higher security risks and face different "threat models" than individuals due to their specific systems used to "store, share, and process user data, as well as the communication platforms, networks, and devices staff and constituents use" to share information.[162]

Digital Literacy

Mainstreaming digital literacy to bring about behavior change is critical to ensure current and future generations are equipped with the knowledge, skills, and tools to detect, deflect, and recover from digital attacks.

Increasing public awareness and promoting digital literacy helps strengthen the public's understanding of how the actions of governments or third parties and how technology works (or does not work) can affect their digital life and rights – positively or negatively. When users become more literate on key issues – such as censorship, surveillance, and content manipulation – "they often take actions that enhance Internet freedom and protect fellow users."[163] In addition, as recommended by UNESCO in the Building Digital Safety for Journalism report (2015), by raising the public's awareness of evolving digital threats, one will organically see an increase in "market demand for digital security tools,"[164] further contributing to strengthening internet freedoms. Likewise, Freedom House's Freedom on the Net 2021 - The Global Drive to Control Big Tech 2021 report states that governments "should invest in digital literacy training through public education, public service advertising campaigns, and other mechanisms to target individuals from all age groups and socioeconomic backgrounds" [165] as a way to address unequal access to the internet, which increases social inequality, and to foster a more diverse information space. According to leading literature, the most common tactics for building digital literacy include: (1) training of trainers and/or educators, (2) creating safe communities of engagement; and (3) providing in-person and online courses or learning platforms.[166] Furthermore, critical to the success of each of these efforts, generating the desired impacts of a digitally literate public, is community-building and coordination of efforts.[167] DRL/GP's respective theories of change align closely with these best practices by deploying resources to build the capacity of human rights defenders, civil society, and other marginalized populations; delivering emergency support services to communities; and, raising awareness across the general public on digital security risks.

However, while "digital literacy is a building block [for Digital Safety]… people hear if you do X, Y, and Z, you'll be protected. And they think that it is absolute. And it is just like one block of what they need to be protected."[168] Toolkits, guidelines, web-based and mobile applications, trainings, and other technology-based applications are necessary tactics and strategies for raising public awareness and improving digital literacy, yet—they are only effective if utilized. "We [need to] move beyond the specific app oriented, training approach, where we think the technology is the thing that's going to solve the problem. It's really going to be behavior change. And behavior change seems to need to be informed by a broad understanding of processes."[169] "Fly-By-Night training is just a thing of the past… And, in addition, in the tech space, the types of threats that any organization are facing change, almost on a day-to-day basis these days. So the idea that any type of one off or even like a couple of trainings might suffice in terms of really being able to provide sufficient understanding and protection just is not realistic when it comes to these types of technologies."[170] To this end, leading SMEs and researchers recognize the need to not only provide a holistic approach to digital safety drawing on nontraditional approaches—but that efforts should also be focused on obtaining buy-in from host country governments and educational programs to mainstream digital literacy within existing adult and child curricula. "It is not a physical threat; someone is not banging down your door. Going through a longer-term educational process was really important for people to understand the threats that they may face in the digital age, and how that could impact their work." [171] "Basic digital literacy [could also be] introduced in public schools, for instance, solv[ing] many of the problems that we are dealing with…[as long as] it is the will of the government and school systems that would accept the basic media and digital literacy curricula …"[172]

ADVANCEMENT TOWARDS IF FRAMEWORK GOAL

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**. The word bloggers here, however, should be interpreted broadly to any Internet user. As the above discussion demonstrates, the sampled grants effectively pushed forward on this goal. Furthermore, the theories of change and underlying assumption that inform the DRL/GP Digital Safety Pillar accurately reflect the historical and evolving nuances of digital security, emergency support, and public awareness raising within the ecosystem.

Localized solutions have contributed to and enhanced DRL/GP's approach and subsequent success around digital safety.

The emphasis on localized solutions in particular arose as a prominent aspect of grantee success toward the IF Framework components and the forward-looking approach outlined by the respective theories of change. 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.[173] Localized solutions—through threat labs, networks of auditors, collaborative conference events—help to expand the number and type of stakeholders involved in the Internet freedom space while delivery tailored training, resources, and other tools. As numerous stakeholders shared, widening the field is essential to strengthening digital security and Internet freedom efforts more broadly.

While DRL/GP's overarching IF Strategic Framework demonstrates its' commitment to a holistic, systems-based approach; the respective theories of change and programs could benefit from further emphasis on these principles.

In particular, SMEs emphasized the value of "going beyond civil society organizations… to a broader set of users of a technology." Similarity another leading expert noted that digital safety is "an area where [DRL/GP and the Internet freedom ecosystem more broadly is] very effective, but at the expense of others. So, for instance, members of the press get a lot of attention on digital security. And the special status they get put in actually exempts them from challenges in other ways."[174] Moreover, "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."[175]

PILLAR 3 POLICY ADVOCACY

Pillar 3, Policy Advocacy, seeks 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..."[176] To achieve this goal, programs under Pillar 3 are designed to foster civil society's potential to effectively engage with Internet policy-making processes, at the local, regional, and international levels, prioritizing the protection of human rights online and democratic values, and pushing them as standards. Moreover, repressive Internet-related policies that undermine Internet freedom can also be challenged by those actors. Such efforts would echo outside the public sector, setting standards and best practices to businesses as well. The following summarizes the overarching goal, embedded values, and lines of effort which comprise the policy advocacy pillar.

THEORIES OF CHANGE AND UNDERLYING ASSUMPTIONS

The Policy Advocacy Pillar is comprised of four lines of effort: (1) Human Rights in Internet Policy, (2) Internet Freedom in Human Rights Policy, (3) Internet Freedom/Business and Human Rights, and (4) Legal Advocacy. Of these four, only two—Human Rights in Internet Policy and Legal Advocacy—were included as part of the evaluation. To assess the effectiveness (EQ 1) and relevancy (EQ 2) of DRL/GP's efforts related to these lines of effort, it is imperative to first understand the perceived pathway of change or theory of change describing how and why a specific or set of interventions are believed to contribute to the desired goal or end result. In addition, it is likewise just as important to understand the underlying assumptions within a given theory of change. Underlying assumptions provide a clear picture of the conditions or resources required for change to occur. Please refer to Annex 5 for DRL/GP's Policy Advocacy Theories of Change and identified underlying assumptions

EFFECTIVENESS OF PILLAR 3

Effectiveness Towards IF Framework Indicators

The Policy Advocacy Pillar contains indicators under two distinct program areas: supporting advocacy and engaging in advocacy. Overall, sampled grants were successful against these program areas, although contextual factors and political changes limited the effectiveness of certain activities under select grants.

DRL/GP successfully supported a large network of civil society actors strengthening their organizational capacity and strategy designs to advocate for human rights.

Program Area 3.1—support advocacy indicators include (1) the number of advocacy interventions supported, (2) the percent of local civil society organizations (CSOs) with improved organizational capacities, and (3) the percentage of local CSOs who have improved advocacy strategies.

The sampled grants under the Policy Advocacy Pillar engaged in diverse interventions to support advocacy and in large part demonstrated effectiveness against these indicators. Eighteen advocacy interventions were supported through small grants under Policy Advocacy Project A; Policy Advocacy Project B secured 97 sponsorships and mentorship partners to facilitate 6 events that engaged a total of 437 participants and generated 106 new innovative ideas related to Internet freedom; and Policy Advocacy Project C reported supporting 21 advocacy interventions through its activities, which included producing 11 State of Affairs reports, hosting regional summits, and disbursing thirteen small grants to support groups engaging in local advocacy.[177]

In many cases, grantees exceeded the planned number of supported advocacy interventions. For example, Policy Advocacy Project B selected 113 teams to participate in organized events out of 382 applicants, significantly exceeding their goal of 30 participating teams.[178] Additional indicators from this and other grants can be found in the table below. While most sampled grants exceeded the planned number of advocacy interventions, one grantee noted that targeting new stakeholders outside the traditional Internet freedom community created a challenge to complete the planned volume of advocacy support interventions. The grant "targeted partners who worked in areas or with groups that had little prior knowledge of Internet freedom issues. Because of this, awareness raising and research was required before advocacy could be undertaken."[179] The need for preliminary awareness raising served as a limiting factor, although it simultaneously aligns the grant with the high-level pillar values (discussed in more detail below).

DRL/GP SUCCESSFULLY ENGAGED OVER

637

CIVIL SOCIETY ACTORS THROUGH DIGIHACKS AND REGIONAL SUMMITS

Table 3. Pillar 3, Performance Against Program-Specific Indicators

Grant	Indicator	Target	Achieved
Policy Advocacy C	Number of advocacy events/ one-on-one sessions administered on Internet freedom through sub-grants	5	32
	Number of advocacy interventions supported by the DRL award	30	21
	Number of policy recommendations presented by advocates and/or lawyers under sub-grants administered	2	57
Policy Advocacy B	Number of teams applying to participate in the event	30	382
	Number of team selected to participate	15	113
	Number of small grant IF-relevant advocacy or technology projects funded	3	12

The additional indicators under this program area reflect the result of advocacy support interventions by identifying the percentage of beneficiary organizations with improved capacities and strengthened strategies. Overall, grants that reported on these indicators demonstrated the effectiveness of the interventions. Grants delivered a diverse range of support, including direct capacity building, networking support, and direct funding through sub-grants. The results of these efforts were universally reported at the level of individual beneficiaries, rather than organizations, but nevertheless demonstrate effectiveness against the spirit of the indicators.

Table 4. Pillar 3, Percentage of Beneficiaries with Improved Capacity

Grant	Percentage of beneficiaries with improved capacity
Policy Advocacy B	95 percent improvement in participants' reported awareness of core themes and opportunities for IF advocacy engagement[180]

Grant	Percentage of beneficiaries with improved capacity
Policy Advocacy C	73 percent of lawyers reported improved familiarity with litigation tactics in Internet freedom-related cases 75 percent of CSOs demonstrated increased knowledge of advocacy tools and methods[181]
Policy Advocacy A	38 percent of beneficiaries increased their advocacy capacity related to Internet freedom[182]

Political challenges and changes in the political climate negatively affected the operating context and limited planned scope and success of some interventions.

For some, this affected singular advocacy efforts under the grant. For example, one of the teams involved in a Policy Advocacy Project B events sought to connect election observers with online tools. Due to "some parallel political events," however, "the government suddenly became really sensitive around this."[183] The online tools were ultimately published but larger and louder advocacy efforts were not feasible at the time. Other grantees experienced systematic challenges. Political changes across Eastern Europe, for example, meant the imposition of significantly greater government oversight and auditing, as well as risk, for local groups. Remaining compliant with local restrictions "really took time away from staff locally to be able to implement projects."[184] Changes in the broader political climate and associated levels of risk to advocates can and did have a limiting effect on some interventions.

Despite challenges obtaining short-term results with supporting advocacy led by stakeholders new to the Internet freedom space, DRL-funded grants directly and indirectly engaged in successful advocacy work that produced tangible changes to laws, policies, and procedures.

Program Area 3.2—engage in advocacy indicators under this program area include number of CSOs that engage in advocacy and the number of laws, policies, and/or procedures that were adopted, revised, stalled, and/or changed to protect Internet freedom. The Policy Advocacy Project A resulted in 14 CSOs (exceeding the target of 10) engaging in advocacy. Many of these CSOs were further "able to establish lasting relationships with governance bodies" and thus continue their advocacy efforts after the conclusion of the grant.[185] Two policies detrimental to Internet freedom were stalled as a result of advocacy efforts completed through the grant. Although the grant did not achieve the target of four policies, this nevertheless reflects success for CSOs who were new to the Internet freedom advocacy space.

Grants engaging in direct legal advocacy under line of effort 12, were highly effective in using the courts to try to counter repressive laws and protect Internet freedom. Over the course of the grant, the grantee handled 313 cases—far exceeding the target of 90 cases.[186] These cases included several significant decisions, including reversing a target government's blocking of Twitter, YouTube, and Wikipedia. Policy Advocacy Project C strategically handled cases in both the respective Constitutional Court as well as in European Courts—"because [the Government] is bound by the European Court of Human Rights, it turns into domestic law as well."[187] These activities speak directly to the indicator regarding advocacy with national, regional, and international bodies.

While some cases are not won in the courts, DRL/GP's advocacy strategy is still relevant for documentation of the problem.

In the case of Policy Advocacy Project C, although "some level of rule [of] law" remains, the grantee goes into many cases knowing "we won't win. The government tells us this."[188] Using the example of criminal cases, submitting applications that the grantee knows will be rejected nevertheless leaves permanent documentation of the cases and to "show the magnitude of the problem."[189] Grantees engaging in direct legal advocacy work reported struggling to use the reporting frameworks and indicators as they did not align well with their work. Reporting against indicators was not always possible and when it was, it may inaccurately reflect a negative result, such as the case of the rejected applications for criminal cases.

Effectiveness Towards Pillar 3 Values

The sampled grants emphasize diverse facets of optimal policy advocacy endeavors. The core values reflected in the sampled grants included the expansion of stakeholders able to advocate, the empowerment of those stakeholders, and the delivery of activities that move beyond capacity building. Through these core values, the sampled grants also embodied the other values included within the Policy Advocacy Pillar. The grants' effectiveness in reflecting these core values is discussed below.

A wide range of local advocacy stakeholders were engaged through the sampled grants, and within specific grants, novel local groups were brought into the advocacy space for the promotion of human rights for a global free Internet.

This was particularly notable under line of effort 9 Human Rights in Internet Policy. Through their promotion and preparation for their events, the Policy Advocacy Project B was able to "engage a new generation of advocates," bringing in new individuals and local groups to both the bootcamp trainings and the hackathon style events.[190]

> In some countries, if you said I'm going to run a workshop on privacy by design, you would be laughed out of the room. But here [...] we used language that was so in parallel with what the government was doing that they couldn't stop it. [...] People who went through the training suddenly had a completely different attitude or understanding of why security by design and privacy in design is important when building technical applications. That is a long-lasting virtue that we managed to inculcate through this process.
>
> DRL/GP Internet Freedom Grantee

Additionally, Policy Advocacy Project B welcomed media coverage to amplify the reach of their events, indirectly reaching additional individuals while expanding awareness of stakeholders with whom they were directly engaged. "The kind of press that these programs got, the kinds of exposure that both advocates and developers received as a result of what was accomplished, was pretty significant."[191] Policy Advocacy Project B's success in promoting and facilitating events to a broad range of stakeholders—and thus taking tech policy into traditionally non-tech HR advocacy spaces by engaging a diverse group of stakeholders—was particularly noteworthy in geographies with more restrictive government policies on Internet freedom. The grantee worked within the parameters of the policies while still promoting and delivering content on key Internet freedom values.

Similarly, the Policy Advocacy Project A actively sought out new organizations to expand the breadth and depth of capable stakeholders involved in the human rights and tech policy advocacy space. Interviewed stakeholders recalled that the grant "always kept the door open to inviting folks that are not already in this space" to identify new groups, or even individuals, who had an interest in advocacy but needed capacity building support.[192] As discussed above with regards to the Policy Advocacy Pillar indicators, this posed a challenge as far as achieving the desired number of advocacy interventions. Nevertheless, the grant captured several success stories of how these identified organizations have since begun—and continued—to engage in advocacy activities. Policy Advocacy Project A "provided capacity building support to numerous organizations, including a volunteer run youth organization. Although the group had "never received a grant before," the project's grantee identified them as an organization of promise and potential. After receiving a small grant and capacity building support, the youth organization is "still actively involved in this space" of internet freedom advocacy today. [193]

Grantees also moved beyond capacity building and implemented activities that promoted strategies for concrete change—a critical value in the Policy Advocacy Pillar.
A common trend across grants was to act as a connector, often between smaller, more local, and/or emerging organizations with larger groups and resources. For example, stakeholders recalled Policy Advocacy Project A serving as a "kind of trusted intermediary" able to put sub-grantees "in touch with organizations, companies, and forums that they maybe wouldn't have access to otherwise, because of power dynamics, and language and all these other things."[194] The grantee could connect sub-grantees with, for example, social media platforms to facilitate discussions about acceptable content and blocked content. Thanks to IF funding, one stakeholder shared, "[Policy Advocacy Project A] has strengthened its position as a trusted intermediary and has built relationships between various partners."

Under line of effort 12 Legal Advocacy, Policy Advocacy Project C successfully created a regional Internet freedom network "from scratch."[195] Although changes in the political climate within specific countries limited the success of the broader grant activities, stakeholders involved with the Policy Advocacy Project C reflected that "creating this network of wonderful enthusiastic partners was an achievement of itself;" the network "created a partnership amongst […] leading organizations on the ground who do Internet freedom work" and use of the network has reportedly continued post-project.[196]

The IF Portfolio, through the sampled grants, effectively implemented the value of advocating at various levels, including locally, regionally, and globally.
Some grants actively engaged in advocacy at local, regional, and/or global levels. Policy Advocacy Project C provided legal assistance and engaged in litigation efforts nationally and regionally, such as through the European Court of Human Rights.

Many grantees indirectly reflected this value by the nature of their work with local organizations. For example, because Policy Advocacy Project A served as an intermediary connecting local organizations with larger groups, they "supported organizations at the local level to take on a more prominent leadership role in conducting" advocacy work.[197] Policy Advocacy Project C developed educational materials, including legislative and jurisprudential guidelines for Internet freedom, that were designed "to inform decision makers, lawmakers on Internet freedom using the knowledge of the sub-grantees to tailor [guidelines] for the local context."[198] Similarly, the Policy Advocacy Project B model actively sought out and supported actors who were uniquely well positioned to identify key local issues and design tailored solutions that were applicable "in the context of the region" they were in.[199] Through resources or networking, grantees offered various kinds of support to enhance the efforts of local groups to engage in advocacy with public and private, national and international stakeholders.

ACCURACY AND RELEVANCY OF PILLAR 3

Challenging Illiberal laws and policies

Advocating for human rights in Internet policy and for legal reforms has and will continue to be a critical component of Internet freedom

Human rights are inherent to all human beings; differences in race, sex, nationality, religion, or any other status or designation do not alter the universal applicability of fundamental human rights.[200] Notably, Internet freedom declined for the 11th consecutive year in 2021, as measured by the annual study under Research Project B.[201] This can in part, be largely attributed to illiberal laws and policies that restrict and/or prevent citizens from exercising their rights online. Thus, advocating for human rights in Internet policy and for legal reforms has and will continue to be a critical component of Internet freedom, validating DRL/GP's theories of change under Pillar 3.

DRL/GP's policy advocacy contributions are widely recognized and valued across the Internet freedom ecosystem. However, DRL/GP may consider prioritizing resources to reflect areas of greatest impact moving forward.

Notably, DRL/GP is recognized by independent SMEs globally as "basically the only donor in the world to invest in [policy advocacy]… 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. For example, getting the UN Human Rights Council to formally acknowledge that online [human] rights are the same as offline rights was much due to DRL partners being able to advocate both locally as well as through the UN Human Rights Council for the recognition of that principle."[202] This example, among others cited by SMEs and grantees alike, demonstrate that not only can illiberal laws and policies be challenged, but that civil society are effective means of bringing about change.

That being said, several SMEs questioned the impact of some policy advocacy efforts, such as legal advocacy, as compared to others, such as advocacy for human rights, acknowledging that the resource limitation and constraints on both DRL/GP and civil society partners. "It is not to say that legal advocacy doesn't matter or that it's not worth challenging illiberal or repressive regulations, it clearly does. But to the extent that we focus on that, rather than a more holistic understanding of what actually prevents people from expressing themselves freely, we often only allow free expression for those who already have really significant material advantages."[203] Furthermore, it is important to acknowledge that the U.S. Government's "interference funding or support for particular types of legal challenges to laws in other countries could get quite complicated." [204]

Legal Advocacy

As reflected in DRL/GP's theories of change, legal advocacy efforts need to acknowledge the context in which they operate to ensure the safety of the targeted communities and to promote the greatest potential for success.

DRL/GP's legal advocacy theory of change makes an important distinction between two very different contexts in which it seeks to operate: (1) countries with an established rule of law where a particular law or policy is considered illiberal or repressive and (2) a country which is fundamentally illiberal. While independent SMEs praised DRL/GP for making this clear distinction, they were found to be more hopeful regarding the success of legal advocacy efforts in the first of the two contexts—in which civil society and activists challenge a particular law or policy enacted by a given country with an established rule of law leveraging an established legal system.

Yet, legal advocacy "is a thing that sometimes works… when you have the right political system, the right legal and theoretical processes, and the actual functioning independence that it is not based on a corrupted or captured judiciary."[205] When operating within a fundamentally illiberal context, one SME pointed out that, "it is very hard to succeed, if the overall architecture, including the legal system is illiberal. [The legal system] is unlikely to be responsive, and to even interpret the laws that exist, as repressive."[206] Similarly, another SME suggested that it is important to acknowledge the context in which you are operating—as well as the topic of the legal issue being challenged—as legal advocacy might be the right approach in one context, but not in another. In an illiberal context, it may be more impactful, as suggested by one SME, for communities to explore mass resistance or mass disobedience and/or tools to challenge illiberal laws. While these kinds of efforts can result in harmful consequences, they "are more effective in the long term than sort of specific kinds of legal advocacy."[207] That being said, as one SME noted, "sometimes you can be surprised."[208] A former DRL/GP grantee highlighted a recent success story in which a sub-grantee led a series of "surprisingly successful legal campaigns in [Southwest Asia] against some repressive digital rights regulations that the government had put forward… in a country that's neither inherently repressive, nor is it a country, I would say, is necessarily rule of law abiding …. Everyone was pleasantly surprised that they were able to achieve success and [the observed] results." [209]

Multi-stakeholder approach

A purposeful and targeted multi-stakeholder approach is key to counter the development of repressive Internet-related laws and regulations.

Under Pillar 3, in alignment with U.S. foreign policy, the respective theories of change assume that a multi-stakeholder approach is critical to achieve the desired results. To pursue the ideal of an open Internet, U.S. foreign policy needs to work via multilateral and multi-stakeholder cooperation and engagement. DRL/GP representative further explained "civil society participat[ion] is what we commonly refer to as a multi-stakeholder process."[210] Evidence supports this assumption, suggesting that successful policy advocacy efforts are understood as communal and multistakeholder[211] undertakings that utilize contextually targeted solutions while leveraging a broader network of support. However, one SME in particular questioned this approach—noting that while it is critical to have a diverse network of stakeholders to bring about change, it is just as important to ensure that the stakeholders are purposively selected and identified to bring about the desired change. The SME went on to explain, that one cannot assume "everybody in civil society is on the same side … there is robust disagreement within organizations that all claim similar goals about how to achieve policies that reflect democratic values and international human rights norms, especially to the extent that we trade off [human rights norms] against each other, for example, privacy rights versus freedom of expression.[212] The SME went on to say that, this is not to suggest that it is not good to support civil society, as civil society has proven to effectively engage in policy making processes, it is rather a "question of which parts of civil society you support" to ensure engagement with the right partners at the right time. [213]

ADVANCEMENT TOWARDS IF FRAMEWORK GOAL

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 evident 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.

> " 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

Employing a multi-stakeholder approach, DRL/GP has empowered a diverse network of civil society to serve as champions contributing to tangible improvements to repressive laws, policies, and procedures.

Throughout DRL/GP programs, including but not limited to those assessed as part of this evaluation, are seen by independent SMEs, other donors, and civil society actors themselves, as having a "huge influence on civil society and human rights."[214] Specifically, DRL/GP has empowered civil society actors by bringing them to the table, where they are receiving "representation in a space that has typically been government corporate technically owned."[215] Importantly, DRL/GP has not only "opened doors" for civil society to be seen and heard among "these kinds of traditionally, either very government or very technical bodies, [civil society is] having actual positive influence on mainstreaming [key] issues… changing the way that some of these governing bodies actually work."[216]

While glimmers of success have emerged, the full impact of DRL/GP's policy advocacy efforts will only be realized over time.

Representative of DRL/GP pointed out that policy advocacy efforts are viewed as a "terminal point" under the IF Strategic Framework. "The outcomes, goals, and end states of policy advocacy… turns out to be a terminal point. [Technology development, digital safety, and research] all feeds into policy advocacy."[217] Thus, it can be assumed that the outcomes and goals of DRL/GP's policy advocacy efforts will only be realized fully, after the goals and outcomes under the other pillars are achieved. Furthermore, the Internet freedom community at large recognizes that overturning repressive laws, policies, and procedures, especially at the government level, are among the most difficult efforts facing the Internet freedom community at large.

PILLAR 4 RESEARCH

The final pillar of the IF Strategic Framework is the Research Pillar. The Research Pillar is designed to carry out research "on key threats to Internet freedom,"[218] including, among other topics, monitoring restrictions imposed by various countries and businesses on Internet freedom and the engagement of Internet users with tools and techniques supported by the DRL/GP IF Portfolio. It also acknowledges the potential of research to raise awareness and provide crucial evidence, expanding the research base of key threats not only within and to civil society, but among and to governments and companies by creating objective and comparable metrics of respect for Internet freedom. Evidence is also seen by grantees and SMEs alike as a crucial source of content for media and the policy advocacy strategies, notably with respect to Pillar 3. The following summaries the overarching goal, embedded values, and lines of effort which comprise the Research Pillar.

THEORIES OF CHANGE AND UNDERLYING ASSUMPTIONS

The Research Pillar is comprised of two lines of effort: (1) Global Rankings and (2) Censorship Measurement. Of these two, only one—Global Rankings—was included as part of the evaluation. To assess the effectiveness (EQ 1) and relevancy (EQ 2) of DRL/GP's efforts related to Global Rankings, it is imperative to first understand the perceived pathway of change or theory of change describing how and why a specific or set of interventions are believed to contribute to the desired goal or end result. In addition, it is likewise just as important to understand the underlying assumptions within a given theory of change. Underlying assumptions provide a clear picture of the conditions or resources required for change to occur. Please refer to Annex 5 for DRL/GP's Research Theory of Change and identified underlying assumptions.

EFFECTIVENESS OF PILLAR 4

Effectiveness Towards IF Framework Indicators

DRL/GP is monitoring the production of evidence on the extent to which countries and companies respect human rights online (indicators 4.1-1 and 4.1-2). While it is unclear the extent to which DRL/GP funded reports are utilized by the public at large, grantees deploy various dissemination tactics to increase accessibility of these reports, including targeted media engagement.

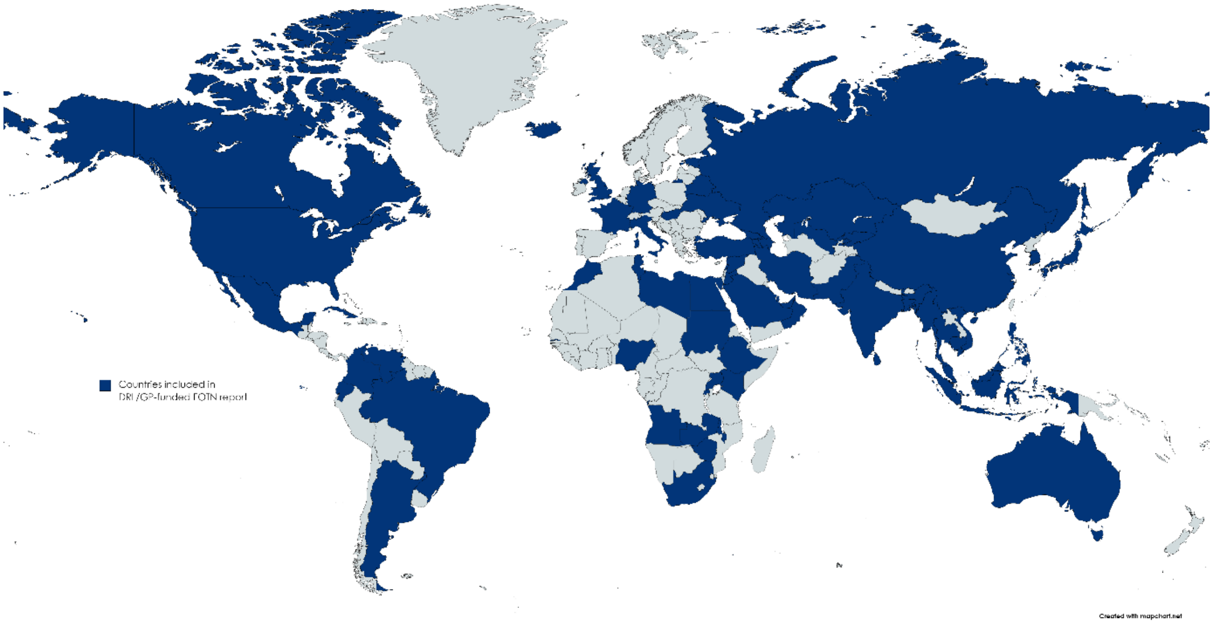
Indicator 4.1-1. Number of DRL IF-supported reports published. Significant amounts of technical reports and content were produced by the sampled grants that exceeded established goals. Across the four editions of the Research Pillar B's report produced from 2016 to 2020, Research Project B generated 260 country reports (65 each year). Funding from DRL supported the research, analysis, and publication of 119 out of these 260 Research Pillar B country reports.[219] Research Project A produced 19 publications, exceeding the goal of 15.[220]

DRL/GP SUCCESSFULLY SUPPORTED OVER

138

PUBLICATIONS UNDER THE RESEARCH PILLAR

Figure 3. Geographic Coverage of Research Project B


■ Countries included in DRL/GP-funded FOTN report
Created with mapchart.net

Indicator 4.1-2. Number of countries where Internet freedom restrictions are monitored. Research Project B has significantly expanded the number of countries included in its report. Since their pilot report in 2009, they have grown from covering approximately a dozen countries to approximately "70 countries, which covers about 88 percent of the world's Internet users."[221] Countries are strategically chosen to maximize coverage of global Internet users as well as diversity of geographies, regime types, and approaches to Internet governance.

Of note are the stories from organizations and experts who collaborated with Research Project B throughout the development of country-specific reports. There is unanimity in that participating in this process, organizations and individuals expanded both their capacity as well as their role as an expert, a monitor, and as an implementer of advocacy and/or research activities for Internet freedom. A local organization assisted in producing one of the country reports and has since shared that their current positions as "one of the go to sources for digital rights in [their country] because they started working on the [annual assessment under Research Pillar B]. They're now one of the conveners of a regional coalition that's aiming at combating digital authoritarianism [across the region]. They're really trusted collaborators of the pro-democracy movement, providing information and resources on Internet freedom to the youth protesters."[222] Through its work, Research Pillar B has indirectly helped to expand the capacity of in-country actors to monitor and work on Internet freedom issues.

Indicator 4.1-3. Number of monthly "user engagements" for DRL IF-supported reports. Neither grantee reported on this standard indicator. Grantees, however, utilized additional indicators to measure the dissemination of research products to key stakeholders, the broader Internet freedom community, and the public at large. For example, Research Project B grantee reported holding launch events around the annual publications.[223] Research Project A achieved significantly more than projected against their additional indicators, as reflected in the table below.[224]

Table 5. Pillar 4, Research Project A, Performance Against Program-Specific Indicators

Indicator	Target	Achievement
Number of languages into which the Index is translated	N/A	7

Indicator	Target	Achievement
Number of public presentations	38	40
Number of media appearances	25	162
Number of international policy fora, debates, etc.	50	100
Number of companies met with to discuss the Index, results, and path to improvement	42	115
Number of companies publicly responding to the Index	16	42
Number of non-English articles about the ranking index written by individuals not associated with the project	8	54

Effectiveness Towards Pillar 4 Values

The values underpinning the research pillar reflect the overarching concept that "research drives everything." In this spirit, the research pillar values include optimizing data for use by multiple stakeholders, ensuring research outputs are open source and for the public good, encouraging the sharing of threat intelligence, promoting effective collaboration, and protecting user privacy and security.

The sampled grants delivered timely research that was relevant to and actively desired by the broader community of stakeholders.

These qualities strongly promote the core value of optimizing data for use by multiple stakeholders. Research Projects A and B products are both increasingly used and referenced by stakeholders to "fight for Internet freedom protections, engage national policymakers, and advocate for positive change."[225] For example, according to a 2020 annual survey implemented by the Research Project B implementing partner, 77 percent of respondents indicated they had used the Research Project B's products in their own recent advocacy efforts.[226] Furthermore, the focus on elections as a flashpoint for Internet freedom restrictions produced "an increase in how companies like Facebook or Twitter or Google have come to [the grantee] around key elections and say, 'Hey, we want to talk with you all. What do you think the major threats are? What should we be aware of? Who should we be talking to in the country? What experts can we talk to in whatever country and can you make those connections?'"[227] Similarly, meaningful discussions have been generated as a result of Research Project A. 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."[228]

The quality and transparency of the methodology and the diverse public engagement and promotion activities helped to raise its profile and increase its use by advocacy actors and also its impact. Grantees agreed that "as we became better known, people were looking forward to our reports and knew how to use them. And we were able to partner with a variety of organizations to promote our work and to build on it."[229]

> Research, standard 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.
>
> DRL/GP Internet Freedom Grantee

That said, one grantee noted that the original technical capacity of some of the local researchers involved could be a limiting factor in producing the country reports. Although the depth and breadth of their research was a strength, the methodological rigor did present a challenging learning curve for some external researchers. In addition, some advocates had a more difficult time understanding "how to get insights from it, how to build advocacy campaigns around it, and so on."[230] Specifically, the legalistic language used to frame many of the normative indicators within the research product can be challenging to interpret and the corporate policies being assessed are themselves "designed to be difficult to scrutinize."[231] Building from this learning, the grantee subsequently devoted additional resources to producing data analysis and explanations to support end users in divining critical and applicable take aways and better embody the value of optimizing data for use.

ACCURACY AND RELEVANCY OF PILLAR 4

Objective and Comparable Metrics

DRL/GP Global Rankings initiatives fill an existing void, contributing to the development of metrics for assessing laws, policies, and procedures that respect human rights online. As described above, DRL/GP has successfully funded programs that have developed metrics—including, for example, Research Projects A and B—where few organizations have the technical and funding ability to develop such assessments. Besides providing a basis for declaring a certain set of conditions as illegal, human rights, these metrics can also be deployed to inform debates and empower CSOs and activists alike through a set of analytic tools for scanning and rating actions of powerful institutions, including governments and technology companies.[232]

> "Research Project B is by far the gold standard, there is nothing better for getting that level of exhaustive, broad, and thorough country level analysis."
>
> DRL/GP Representative

Metrics or "indicators" are widely perceived to be useful tactics, yielding accurate and applicable research to support human rights advocacy efforts. Metrics or indicators, such as Research Projects A and B, are proven to support the measurement and assessment of, for example, the extent to which rights are being fulfilled or enjoyed in a given situation.[233] "These rankings are effective at changing the behavior of the actors being ranked, be they countries, companies, or other entities."[234] Exposing the specific areas of where a given country or company is lacking can inform advocacy strategies targeting stakeholder groups such as a companies' clientele and even their board members. Having access to these metrics and a given country or company's compliance with human rights can be a powerful negotiation and advocacy for change tool, especially if the results in comparison are unfavorable.[235]

Notably, while limited in number, there are a handful of other, likeminded reputable metrics or rankings in the Internet freedom ecosystem—SMEs mentioned for example, the World Benchmarking Alliance Digital Inclusion Benchmark, Reporters Without Borders World Press Freedom Index, and the World Wide Web Foundation Web Index. The continued investment in these metrics signals that these respective donors also see global rankings as an entry point to persuade policymakers, communicate with stakeholders, convince funders to support a certain approach, educate journalists, and impact public opinion, further validating DRL/GP's assumption that global rankings can bring about change.[236]

Despite broad consensus across donors, stakeholders, and SMEs of the value of these metrics to protect universal and unalienable human rights, the notion that these metrics are objective was questioned by some.
While Research Projects A and B are grounded in international standards, established and codified in international institutions and mechanisms, notably the International Covenant on Civil and Political Rights—several SMEs challenged the use of "objective." SMEs suggested, as part of a broader discussion around international development—that is imperative that donors, such as DRL/GP, among others, continually acknowledge that these metrics may, in part, be normative. "We imagine an ideal or an aspirational form of rights and somebody's doing that imagining."[237]

Furthermore, while metrics can be extremely valuable, they are also hard to develop and even more challenging to develop with methodological rigor to allow comparability.
This is especially true for digital rights-related advocacy, where methods for investigating the Internet's policy effects, Internet users' behavior, and corporate decision-making are often highly technical, sensitive, and ever-changing.[238] In digital rights research, the research products that have emerged over the years usually rely on composite information, with the general purpose of providing both individual assessments and allowing for a comparative analysis of the actors they map with respect to rights such as privacy and freedom of expression.[239] That being said, SMEs noted that "there tends to be a causation correlation problem in this space… or often a false equivalence."[240] To address these challenges, over the years, grantees become more transparent about and exploit in their methodologies.

Despite this concern and acknowledgement that this has been an issue in the past within the ecosystem more broadly, SMEs all agreed that **the products produced under Research Projects A and B were among the most rigorous and widely respected "powerful levers" for change**.[241] One subject matter expert in particular noted, "whenever we work in a new country, we always go and check these sorts of things [Research Pillar B], or whether we're looking at a new vendor or company to use, we look" to Research Project A.[242] Relatedly, another informant reflected on the Research Project B, saying, "the project is by far the gold standard, there is nothing better … for getting a certain level of exhaustive and broad, thorough country level analysis."[243]

Accessibility and Advocacy

Civil society and human rights defenders represent just one group of users who do and could access and employ global rankings for human rights advocacy.
DRL/GP's Global Rankings' theory of change targets civil society and human rights defenders as advocates for change, with a focus on advocacy at the country and company levels. While civil society actors and human rights defenders are and have traditionally been recognized as valuable champions for change, several SMEs questioned whether they are the best positioned to bring about sustainable and scalable change, particularly at the country level. Furthermore, SMEs voiced their opinions in that civil society actors are not the only champions in the Internet freedom ecosystem cultivating change. Consumer activism, for example, is a powerful tool to employ against companies and corporations who commit human rights violations. By employing consumers, one can incentivize regulators, policymakers, and markets to signal "better behavior that is better for human rights."[244] Moreover, companies can also leverage their influence to persuade government and state actors to adhere to human rights online. It is imperative that donors, including DRL/GP think not only about how the metrics are constructed, but also, who their target audience or "client [is] for this type of work. [And how these metrics] actually get into the right hands and seen by the right people."[245]

While DRL/GP uses various platforms and products to promote access to global rankings, it is unclear how the target actors are to access and utilize these metrics.
As discussed above, DRL/GP's grantees acknowledge that some of the target stakeholder groups, mainly local and community-based advocates, find it difficult to "get insights from [their products]" and cannot readily "build advocacy campaigns around it…."[246] One SME expressed similar views noting that while these DRL/GP-funded products are "very useful benchmark[s] of how different countries [and companies] compare. I'm not entirely sure how it's contributed to better policymaking specifically."[247] Building on this, another SME reiterated the question as to who these tools were designed for and how were they intended to be used by the target audience. Relatedly, they pointed out that the existing theory of change does not describe how civil society and human rights defenders will use these metrics to bring about change for greater respect of human rights online once these metrics are made available to the Internet freedom community.

> "DRL [could] think not just about building the rankings, but also about what their market is essentially, who is the client for this type of work… there is a whole bunch of advocacy that needs to happen for this work to actually get into the right hands and seen by the right people."
>
> Independent SME

The pathway to advocate for greater human rights online differs when targeting companies as compared to countries.
While DRL/GP Global Rankings' theory of change allows for flexibility in approaches and practices, the simplicity of the identify pathway for change does not explicitly acknowledge the unique incentives and constructs of bringing about change at the country and company levels. SMEs pointed out that when ranking companies as a tool to strengthen policies and procedures that respect human rights online, it is critical that advocates acknowledge that companies are incentivized by "regulation [and] return on their profit. There's also broader consumer behavior and preferences and activism, which will also influence companies…."[248] In contrast, there are many more levers available to motivate change at the country level, making it "harder to bring about change through something like [Research Project B] than it is through company rankings." [249]

As a result of these nuances, SMEs saw significant value and the greatest potential for impact in deploying rankings at the company level.
One stakeholder in particular noted, "companies are the intermediaries for human rights abuses, frankly, [they] are enablers [who] don't regard themselves as being particularly responsible. [Companies] think their presence in a country as being tantamount to… taking on responsibility for protecting and enacting human rights standards… because they get to continue to operate in a repressive country, as if we should be grateful to them, because they're there at all."[250] Building upon this, another stakeholder pointed out that global rankings "can work for companies because it plays with existing mechanisms, like the idea that we're only going to invest in companies that are doing the right thing around human rights, right? There's a whole socially responsible investment strategy that that can play into."[251]

> "We definitely saw some direct impact… for example, the evaluation of [a company] was used by shareholders to develop a resolution calling for [the company's] human rights policy to be more transparent around freedom of expression. And that contributed very directly to changes that [the company] made in their policies."
>
> DRL/GP Internet Freedom Grantee

ADVANCEMENT TOWARDS IF FRAMEWORK GOAL

Ultimately, the goal of the Research Pillar was to **research key threats to Internet freedom**. As the discussion above demonstrates, the sampled grants effectively pushed this goal forward, delivering timely and relevant information to stakeholders about core Internet freedom issues. 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.

> “[Research Project B] is by far the gold standard, there is nothing better for getting a certain exhaustive, broad, and thorough country level analysis. It's absolutely the gold standard.”
>
> DRL/GP Representative

The uptake of the produced methodologies and associated research products illustrate the advancement of the goal.

Research Project B is perceived by many as a gold standard, as discussed above, and Research Project A has moved the needle in discussing corporate responsibilities for protecting human rights online. Each year, the Research Project A, for example, was cited in leading literature over 200 times. And this number only continues to grow. With respect to Research Project B, “we've seen over time that companies have been gradually improving their scores, both because we directly pressure them to do so and give them a very specific roadmap […] But also because we've served a norm setting function, where other organizations that are making the same ask of companies, point to us and say, it's an expectation that's set in the Research Project A methodology. This is, you know, we're not the only people saying you should do this thing. This is an accepted norm. So we've been very successful in gradually changing company disclosures about their policies and practices over time.”[252] Although it can be difficult to prove causality—“companies do not want to say that they are making changes in direct response to advocacy”—it is clear that the research products funded by DRL/GP are informing and shaping the discussions around key threats to Internet freedom.[253]

RECOMMENDATIONS

While the Internet freedom ecosystem has developed extensively over the past decade—in large 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 support DRL/GP's forward motion and leadership across the Internet freedom ecosystem, the evaluation team suggests the following recommendations for DRL/GP's consideration.

Effectiveness, Accuracy, and Relevancy of DRL/GP IF Strategic Framework

Recommendation No. 1: Sensitize grantees, among other key stakeholders across the Internet freedom ecosystem, on key terms and concepts of DRL/GP's vision for success.
Across all four Pillars grantees and SMEs expressed a need for further explanation of how DRL/GP was utilizing specific terms and concepts. Moving forward, DRL/GP could consider reflecting upon the existing theories of change and underlying assumptions to provide public facing definitions for key terms. For example, terms such as bloggers, human right activists, human rights defenders, and illiberal laws, among others, were questioned by grantees and/or SMEs during data collection. Notably, illicit use and safeguards were among the two top terms that required further explanation as to how DRL/GP defined and viewed these concepts. Providing grantees first and foremost with these definitions will offer clarity to expand their understanding and better equip them to proactively incorporate an awareness of how their program design participates in a strategy of mitigation of illicit use. Upon clarification during the data collection process, for example, one grantee from a VPN-like tool suggested that they use their agency in their network to avoid opening ports to illicit content or action. Encouraging grantees to consider and address illicit use independently, outside of the procurement process, does come with its own risks. Uninformed safeguards can introduce vulnerabilities in the technology which make them less effective or create security risks for the communities they aim to serve. To combat this any public-facing definitions of illicit use which may be used by grantees in proposal development should be accompanied by a general method of subjective evaluation they can use to try and balance safeguards they are considering.

Recommendation No. 2: In addition to defining key terms and concepts as part of the IF Strategic Framework, DRL/GP may consider formalizing an overarching IF Monitoring, Evaluation, and Learning plan.
While DRL/GP has established key components of a Monitoring, Evaluation, and Learning (MEL) plan—including theories of change and performance metrics, the evaluation team was unable to access a comprehensive plan summarizing DRL/GP's overarching approach to monitoring, evaluation, and learning. The lack of a formal MEL plan may have contributed, in part, to inconsistencies in how grantees across all four pillars monitored their performance. 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. As a result, DRL/GP is left with an incomplete view of how funds have been deployed and the effectiveness of the funded programs. 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.**

Recommendation No. 3: Conduct a gap analysis to expand the IF Strategic Framework to address funding gaps and needs within the ecosystem to further Internet freedom.

While the Internet freedom ecosystem is well established—largely in part due to DRL/GP efforts—the ecosystem still requires funding. 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. For example, donors often look to support the development of new and emerging technologies—looking for the newest innovation. However, DRL/GP and SMEs recognize that there are numerous technologies that have proven to be effective that rely on continued support to sustain and scale their efforts. This gap in the funding space led DRL to develop and launch a new Multilateral Surge and Sustain Fund for Anti-Censorship Technology in 2022. This fund will support existing critical and effective censorship circumvention technology platforms, and help them scale to connect more users to the uncensored Internet and sustain these connections in times of greatest need.

Based on SME and grantee feedback, DRL/GP may consider the following preliminary recommendations as potential areas of focus looking ahead:

- Invest in disseminating best practices of the tool rather than prohibitive behaviors.
- Explore way to strengthen the sense of community ownership over tools that target very niche audiences or organizations. In addition to enhancing accessibility, creating a sense of community ownership could minimize the risk of illicit use as a whole "community" is monitoring the tools' usage.
- Expand target communities to include greater emphasis on nontraditional champions or actors for change, for example, companies and universities particularly with respect to policy advocacy and digital safety, respectively.

In addition, to the extent possible, DRL/GP may consider extending the length of funding, particularly for programs that have strong evidence proving their effectiveness. Many grantees pointed out that it is quite difficult to respond to the dynamic and complex challenges they face knowing that their partnership with DRL/GP is often limited to a few years.

Recommendation No 4: Continue to review and update theories of change to reflect the ever-evolving context of the Internet freedom ecosystem.

Across the board, the evaluation findings indicate that DRL/GP's theories of change and underlying assumptions are grounded in evidence and international best practices. Independent SMEs and grantees alike reaffirmed and validated the accuracy and relevancy of DRL/GP's perceived pathways of change. Recognizing that DRL/GP routinely reviews, questions, and updates the IF Strategic Framework, the evaluation team would like to encourage DRL/GP to continue this practice and explore the following considerations as the Internet freedom ecosystem is one which constantly evolves and changes.

- **Pillar 1: Technology Development**
  - Expand the Pillar 1 theories of changes to reflect the potential impact that the broader and evolving context of digital repression—mainly Internet governance—could have on the success of anti-censorship and secure communication technologies.
  - Expand the Technology Pillar target audience—largely the Secure Communication and DDoS mitigation theories of change—to also include citizens in repressive environments.
  - Expand the existing theories of change to recognize that marginalized populations, often times, do not have access nor the agency to use the devices required for Internet freedom related technology—as well as the associated unintended consequences that may result from such use.

- **Pillar 2: Digital Safety**
  - Consider prioritizing capacity building efforts that target change at the organizational level.

  - Explore new and innovative approaches to capacity building—including, for example, collaborating with host country governments and educational programs to mainstream digital literacy within existing adult and child curricula.

- **Pillar 4: Global Rankings**
  - Expand the target audience or intended users of Global Rankings products beyond civil society and human rights defenders to include the consumers of goods, for example.
  - Expand the underlying assumptions to pinpoint how the target actors are to access and utilize these metrics.

EMPLOYING EFFECTIVE SAFEGUARDS TO MITIGATE ILLICIT USE OF DRL/GP SUPPORTED TECHNOLOGY

Recommendation No. 5: Update and expand the IF Illicit Use Mitigation Strategy to more clearly articulate the process that is implemented throughout the grant cycle.

The evaluation team's assessment of the established safeguards was restricted, in part, due to limited access to available documentation to clearly understand DRL/GP's efforts to mitigate illicit use, particularly with respect to the Internal Risk Assessment Form. While the team was able to identify a series of applicable risks and corresponding safeguards across the grants pre-selected by DRL/GP to include in the evaluation, the evaluation team was unable to verify if these risks were of the same as those identified at the procurement phase and during subsequent annual assessments conducted by DRL/GP's experts. In light of this, DRL/GP should consider reviewing, updating, and expanding 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. Based on the evaluation teams understanding of the process—DRL/GP may consider expanding upon the current strategy to further strengthen its approach to mitigating illicit use as follows:

- Expanding the GOR Analysis Template to document how DRL/GP understands the proposed technologies to align and promote the human rights use case, including how the technology will be developed with a human centered design targeting a specific audience, demonstrating alignment with DRL/GP core safeguards and standards.
- Expand the IF Illicit Use Mitigation Strategy to document the process of how technologies are assessed during the procurement phase to identify potential risks of illicit use. DRL/GP could consider drawing upon external, independent SMEs to validate the risks identified across a short list of potential grants prior to award.

Recommendation No. 6: Intentionally and strategically collaborate with grantees under Pillar 1 to enhance the effectiveness of safeguards to mitigate illicit use.

While grantees across all four pillars acknowledged that DRL/GP is both supportive and proactive despite limited resources, it would behoove DRL/GP to expand their existing collaboration with Pillar 1 grantees to sensitize them on the process and importance of establishing effective 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. Collaboration with grantees could also provide more opportunities for grantees to exchange ideas and share knowledge among themselves and the DRL/GP team, identifying synergies between programs and increasing DRL/GP's impact.

ANNEXES

ANNEX 1. EVALUATION SCOPE OF WORK

The DRL/GP Internet Freedom (IF) team anticipates awarding one contract to conduct an evaluation to understand the outcomes of activities conducted throughout the IF portfolio. The IF Team manages over 50 active programs in every region of the world, with a special focus on countries where there are severe or emerging restrictions on freedom of expression and assembly or privacy online. Users in such countries or contexts often face extensive online surveillance and both legal and technical restrictions on their freedom of expression, which may include violence and criminal reprisals as well as blocking of content or access to the global Internet. DRL programming responds to these challenges in accordance with the mandates of the Consolidated Appropriations Act and the US National Cyber Strategy. The objectives of this evaluation are to: (a) establish the effectiveness of current programming strategies in meeting objectives and goals (b) explore implementation lessons that can be applied in future programming (c) determine the status of outputs and outcomes corresponding to program objectives against standard indicators; and (d) ascertain any unintended outcomes of programming. The purpose of this evaluation is to provide the IF team with data on which strategies should be continued, discontinued or adapted in future programming to facilitate success in meeting objectives, minimize risk of unintended outcomes, and develop publicly available information on the program and the extent of its effectiveness.

BACKGROUND

DRL's mission is to advance human rights—including internet freedom—democratic institutions, and fundamental freedoms abroad with the aim of ensuring a more peaceful, prosperous and stable world. Through its IF programming, the DRL Office of Global Programs aims to achieve Bureau Goals, and associated Mission Objectives, within its Functional Bureau Strategy including:

Bureau Goal 3: Increase respect for human rights and fundamental freedoms, both online and offline.

- Objective 3.1: Persuade governments to end serious abuses of human rights, including torture, extrajudicial killings, disappearances, censorship, criminal penalties for peaceful expression, restrictions on free association and peaceful assembly, and undue restrictions on independent media.
- Objective 3.2: Increase capacity of partners and allies to ensure government institutions and security forces do not abuse the rights of citizens.
- Objective 3.3: Defend human rights standards internationally to ensure they remain consistent with American values.
- Objective 3.4: In partnership with the private sector, strive for global standards that promote responsible business conduct, maintaining a level playing field for American businesses as they respect human rights and fundamental freedoms abroad.

In line with the Section 7050 of the Consolidated Appropriations Acts of 2020 and 2021, IF programs are funded 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;
- Combat violence against bloggers and other users;
- Enhance digital security training and capacity building for democracy activists;
- Research key threats to Internet freedom;

- Continue 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; and
- Maintain the technological advantage of the United States Government over such censorship techniques.

IF programming also aims to meet the 2018 US National Cyber Strategy goals of:

- Protecting and promoting an open, interoperable, reliable, and secure Internet and ensuring that this approach to an open Internet is the international standard and;
- Preventing authoritarian states that view the open Internet as a political threat from transforming the free and open Internet into an authoritarian web under their control, under the guise of security or countering terrorism.

In drawing from the aforementioned DRL Functional Bureau Strategy, Consolidated Appropriations Acts, the 2018 US National Cyber Strategy, the existing IF strategic framework focuses on four pillars of programming. These pillars are Technology Development, Policy Advocacy, Digital Safety, and Research. IF programming aims to embody the following values and goals in its programming:

- Protect and promote an open, interoperable, reliable, and secure Internet.
- Protect the online exercise of human rights and fundamental freedoms such as the freedoms of expression, association, peaceful assembly, religion or belief, and privacy rights online.
- Work to ensure that our approach to an open Internet is the international standard.
- Protect vulnerable and marginalized voices.
- Do no harm.

The evaluation team should draw on the strategic frameworks outlined above as well as the IF Strategic Framework and standard IF indicators to meet the objectives of the evaluation.

EVALUATION QUESTIONS

In order to meet the objectives of the evaluation, the evaluation team will answer three evaluation questions. The first two questions include the scope of programs throughout the four pillars of IF programming. The third evaluation question, regarding the use of IF-funded technologies for illicit use, is only focused on programs within the technology development pillar and should be approached as an independent question. The three evaluation questions are:

1. How effective are IF programs completed within the last five years, as assessed against the IF Strategic Framework indicators, values, and goals?

2. How accurate are the assumptions that form the basis of the IF Strategic Framework Lines of Effort?

3. 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?
   a. Which safeguards have not been effective among these?
   b. What are other effective safeguards that DRL Internet Freedom team should consider utilizing to minimize IF-funded technologies for illicit purposes?

To assist the offeror in their drafting process, DRL has included an illustrative list of a few DRL awards within each Internet Freedom program pillar. The below programs are representative of the four pillars and have budgets ranging from $750,000 to $2,000,000:

IF Pillar	Location	Overview	Project Dates
Research	Global	The objective of this program is to safeguard human rights online by empowering local and international stakeholders with the tools and expertise necessary to systematically track internet freedom and advocate against restrictive practices and policies.	July 2016 – December 2020
Technology Development	Global	The objective of this program is to support human rights and democracy by giving mobile users in the Global South an easier way to access uncensored Internet content and services without fear of surveillance by building a Tor Browser for Android.	July 2017 – December 2020
Digital Security	Global	The objective of this program is to improve the user experience of core privacy, security, and anti-censorship tools to increase adoption of digital safety tools by at-risk groups and marginalized communities.	August 2015 – October 2019
Policy Advocacy	Global	The objective of this program is to increase the institutional capacity of civil society organizations to engage effectively in Internet freedom advocacy to support human rights online.	June 2016 – December 2018

EVALUATION DESIGN AND DATA COLLECTION METHODS

Proposed methodologies must employ mixed methods which aim to gather both qualitative and quantitative data. The sampling frame includes 88 IF programs worldwide that have a period of performance between 2015 and September 2021. The proposed sampling method must incorporate the need for the sample to be representative of programs operating in each pillar and nine (9) Lines of Effort (LOE) of the IF strategic framework. The sample will therefore be made up of at least 27 programs.

The evaluation may employ two different methodologies; one to answer the first two evaluations questions and a second for the third evaluation question. While DRL does not have a preference for the outcome evaluation design, vendors must provide a clear rationale for proposed methodologies, such as outcome harvesting or multi-level analysis. In addition, proposed methodologies must include data collection methods (archival collection, semi-structured interviews, etc.), data collection tools (online surveys, data scraping, etc.), data analysis techniques (thematic coding, explanatory, etc.), evaluation design's validity, and triangulation methods of findings. Each item within the methodology should include the reason these design elements were chosen and why they are most appropriate to answer the evaluation questions.

EVALUATION TEAM REQUIREMENTS

The Contractor shall form an expert team consisting of one senior evaluation expert and one mid-level evaluation expert, as well as one project manager and one junior support staff, and relevant in-country consultants, if applicable. However, there is flexibility to propose an alternative staffing structure with proper justification, if the Contractor feels it is more appropriate. The following includes illustrative profiles of background and experience DRL seeks from the Contractor.

1. Evaluation team with knowledge of and expertise in the evaluation of foreign assistance projects, which is to include projects focusing on Internet Freedom. The evaluators should have specific relevant technical expertise or experience that informs a broad understanding of 1) research and policy advocacy related to protecting freedom of expression and privacy online, 2) digital security best practices and methodologies for vulnerable and marginalized populations in repressive online contexts, and 3) technical methods and tools for circumventing, mitigating, or measuring online censorship in various forms, as well as the potential application of these methods and tools for other purposes. Experience should include regular past engagements with Internet Freedom programs across the aforementioned categories. DRL encourages applicants to consult with other Internet Freedom program funders, such as the Open Technology Fund, to identify evaluators with appropriate experience. The team must also demonstrate strong and prior experience evaluating U.S. government or other donor programs addressing human rights issues preferably in sensitive environments. Evaluators can be based outside of the United States and the team should include strong local knowledge in the selected contexts.

2. Capability with methods for virtual data collection that allow for secure communication and data storage.

3. Experience with a variety of evaluation methodologies appropriate for this assignment, particularly outcome evaluations. The ability to analyze, synthesize and draw conclusions and lessons learned from various sources of data and findings.

4. One program manager / senior evaluator (Evaluation Methods/Implementation Specialist – Senior): will be responsible for managing the overall evaluation effort, to ensure that all deliverables are provided in a timely manner and are of sound quality. The senior evaluator will be responsible for preparing the evaluation design, proposed methodology, and data collection instruments. They will be responsible for overseeing the work of the mid-level evaluator(s), including desk review; data collection, such as key informant interviews; and, data analysis. If necessary, the senior evaluator may accompany the mid-term evaluator(s) with data collection. The senior evaluator will also be responsible for preparing and managing the drafting of interim and final reports / deliverables; and, preparing briefings to be provided to DRL and partners. The senior evaluator must be comfortable working in close coordination with DRL, implementing partners, government officials and other donors, and project participants and beneficiaries; and, must possess exceptional organizational and communication skills. The senior level expert should have a minimum of 8 years of designing and implementing evaluation research, including experience leading an evaluation team. The senior level should have a demonstrated ability of evaluating foreign assistance programs addressing human rights issues. Strong preference is given to individuals with experience conducting evaluations in restrictive settings and with marginalized populations. The level of effort for the senior level experts should be no more than 155 person days.

5. One mid-level evaluators (Evaluation Methods/Implementation Specialist – Mid): will be responsible, with the senior evaluator, for conducting and coordinating the overall evaluation effort, including the preparation of the evaluation design and methodology and data collection instruments. The mid-level evaluators will be primarily responsible for conducting the desk review, key informant interviews (KIIs) or other data collection, conducting data collection, data analysis, writing the draft and final reports, and assisting in the preparation of the briefings to be provided to DRL and partners. The mid-term evaluators must be comfortable working in close coordination with DRL, implementing partners, government officials and other donors, project participants, and beneficiaries. The mid-level evaluators should have a minimum of 4 years' experience in monitoring and evaluation (M&E). Preference is given to candidates that have shown a demonstrated ability to design and evaluate foreign assistance evaluations addressing human rights issues, including experience working in restrictive settings and with marginalized

populations. Must possess exceptional organizational and communication skills. The level of effort for the mid-level evaluators should be no more than 199.5 person days.

6. One Project Coordinator (Administrative Support – Junior): The project coordinator will be responsible for providing overall administrative and logistics support to the evaluation team during each stage of the evaluation. The level of effort for the project coordinator should be no more than 44 days.

7. One Communication Specialist – Mid or Junior: If needed, the Contractor may employ a communications specialist / graphic designer for this assignment. This expert will provide guidance to ensure all deliverables are appropriate for each audience and visually appealing. The level of effort for the communications specialist should be no more than 11 days.

ACTIVITIES TIMELINE

Evaluation Design

- Within two weeks after signing the award, the Contractor will meet with DRL for an initial kick-off meeting and handover of materials. Two months after this initial meeting, the evaluation questions should be further refined, if necessary, and a draft inception report of the evaluation should be submitted. The inception report should contain the following: evaluation design and methodology; evaluation questions; theory(ies) of change and underlying assumptions for the projects; information to be analyzed and the respective information sources; work plan and timetable for data collection; and conditions and capacities necessary for data collection, analysis and communication of findings. The evaluation design phase may also be conducted collaboratively with DRL, implementing partners, and other funders and stakeholders.

- The Contractor shall provide all evaluation instruments (e.g., survey questions, interview protocol, focus group protocol, list of stakeholders to be interviewed, etc.) and documentation (e.g., correspondence, contact letters, data collections instruments, fieldwork reports, etc.) to DRL for review and clearance prior to disseminating to participants and key stakeholders. When forming a work plan and timetable, please account for a 2-week feedback period.

- It is the Contractor's responsibility to identify and describe data collection mechanisms based on experience and expertise, keeping in mind security and confidentiality issues. This assignment will require virtual / remote data collection; thus, the Contractor should be familiar with secure digital tools for interviews, focus groups, surveys, etc.

- Data collection methods may include document review, surveys, structured and semi-structured interviews and focus groups, observation, and any other appropriate methods. As a portion of this evaluation is retrospective, the Contractor may propose alternative methodologies (e.g., outcome mapping, causal-comparative study, comparative case studies) that can clarify how process and context affected the results of interventions. Data collection, at a minimum, should include relevant DRL staff, implementing partners, and project participants and/or beneficiaries.

- Other funders and stakeholders not formally associated with these projects should also be included as a means of providing context and determining how these projects fit within the larger framework of IF funding. DRL will facilitate contacts with other funders over the course of the consultation phase. The Contractor shall inform DRL when data collection has been completed.

Data Collection, Analysis and Reporting

- As a fundamental principle of DRL's operations with these projects is "Do no harm," it is vital for the Contractor to work very closely with DRL to determine how to gather accurate and reliable data from participants and key stakeholders in a manner that does not damage trust or jeopardize the safety and security of implementing partners, beneficiaries and communities, data, or the projects themselves. Additional time should be incorporated into the timeline to address this concern in the evaluation design and data collection phases.

- **Desk review and Literature Review:** The Contractor shall conduct a desk review for the sampled programs. At a minimum, this review will include a review of available solicitations (requests for proposals), grant proposals, grant agreements, quarterly progress reports, final project reports and project evaluations. This may include trip reports and internal grant reviews conducted by DRL Program Officers. The desk review should also include other materials that provide information on global trends related to internet freedom programming. The literature review will contain a summary of relevant existing empirical evidence (both academic and grey literature) on the theories of change currently employed in IF programming.

- **Preparation:** Depending on COVID-related security measures, activities will include interviews in Washington, D.C. and/or remote interviews to prepare for data collection with grantees and beneficiaries. Washington, D.C. interviews: Time should be allotted for meetings with relevant offices, agencies and organizations in Washington, D.C., including DRL, implementing partners, and others to gain a greater understanding of DRL and other human rights funders. Remote interviews with key stakeholders: project participants and beneficiaries, implementing partners and their stakeholders, and other funders and experts not affiliated with these projects. DRL can make introductions to DRL implementing partners, relevant Embassy staff, and other stakeholders (funders, non-profits) abroad, if necessary. The Contractor is responsible for handling logistics for data collection and travel. Additionally, the Contractor is responsible for forming research partnerships with local firms or consultants, if necessary.

- **Data Collection:** The Contractor will be expected to conduct data collection with various methods, including virtual and remote methods when appropriate. Specific countries and projects of focus will be identified collaboratively between DRL, its implementing partners, and the Contractor. Depending on the nature of the projects, data collection may include virtual interviews or focus group discussions, remote surveys or other appropriate methods with those in-country. Security protocols for virtual data collection should be determined collaboratively between DRL, its implementing partners and the Contractor. DRL expects the Contractor to include information gathered from project beneficiaries, grantee local staff, grantee local partners, and key stakeholders where feasible. Where interview subjects have relocated, DRL or grantees can assist in locating these subjects and making the introduction for further data collection. DRL can make introductions to implementing partners and relevant staff, but the contractor is responsible for handling data collection logistics. If needed, the Contractor is encouraged to collaborate with an in-country consultant to assist with data collection, analysis, and validation. Contractors may need to include linguistic interpretation.

- **Data Analysis:** Once all data has been collected, data analysis should be completed within two months. The presentation of preliminary findings should take place in Washington, D.C. or virtually with DRL, and then with implementing partners, within a month of completing the analysis.

- **Reporting:** Within one month of the presentation of the preliminary findings the initial draft report should be submitted to DRL as a deliverable. For each draft, approximately two weeks should be planned for feedback from DRL, implementing partners, and other stakeholders. The Contractor shall plan on approximately two draft versions of the report / deliverable for feedback. Draft versions should be free of errors: grammatical, typographical, and analytical. DRL will undertake a final review of all changes to the reports before the Contractor makes multiple final hard copies. The Assistant Secretary for DRL has authority for final approval and release of all final reports.

DELIVERABLES AND TIMELINE

Work on this evaluation will begin on the date the task order is signed.

The following list includes an illustrative timetable; however, the Contractor may propose alternatives, with proper justification. All report deliverables should be formatted to comply with Section 508. The contractor shall provide the following deliverables to DRL:

- **Monthly Progress Reports:** Within the first 10 days of each month, the Contractor will submit a written progress report to DRL. The Contractor will also hold weekly phone calls with DRL, as needed. The agenda of the call will be set by the Contractor prior to the meeting. The Contractor and DRL may cancel calls if the work is progressing and there are no items to discuss. The Contractor shall maintain open, timely, and effective communications with the COR (to be determined), resulting in a relationship that proactively addresses potential problems with flexible, workable solutions. If delays or extensions are needed, please provide this notice as a written request. All correspondence of this nature, and any correspondence seeking acceptance of deliverables, should include the COR for this project.

- **Inception Report (including detailed work plan and evaluation design):** Within approximately 60 days from the kickoff meeting, the contractor will present to DRL an inception report for the evaluation. This document will include a work plan and timetable, evaluation design, methodology, data collection instruments and IF theories of change. DRL, implementing partners and other stakeholders shall be provided an opportunity to review the draft plan and propose evaluation activities or processes; please account for drafts and feedback within this time frame.

- **Desk and Literature Review:** Within approximately 30 days of the approval of the inception report, the desk review and literature review will be completed and a written literature review will be submitted. These reviews may begin as the Contractor drafts the inception report.

- **Data Collection:** Data Collection should be completed within 120 days of approval of the inception report.

- **Draft Evaluation Report and Deliverables:** Within approximately 8 weeks from the completion of data collection, data analysis will be completed. Within approximately 6 weeks after the completion of the aforementioned data analysis, the Contractor will submit a draft report / deliverable. The Contractor will provide an oral briefing to review the draft evaluation report with DRL and partners.

- **Final Evaluation Report and Deliverables:** The contractor will submit the final report within 21 days of an oral briefing on the content of the final evaluation report / deliverable. The final evaluation report should include the following:
  - Internal evaluation summary of no more than three pages. This document serves as a brief for senior managers and policymakers. It provides a brief description of the portfolio evaluated, data collection methods, key findings and recommendations.
  - Internal evaluation report of no more than 75 pages (not including appendices) that presents findings and draws conclusions based on the analysis of evidence. The report should be clear, concise, and empirically grounded.
  - External evaluation report or other deliverable (e.g. slide deck) of no more than 50 pages (not including appendices) that presents findings and draws conclusions based on the analysis of evidence.

The report should be clear, concise, and empirically grounded. This version of the report may be posted on the Department of State evaluation clearinghouse if it is not deemed sensitive. It should be ready for publication upon receipt, and should not include sensitive information or disclose the names of implementing partners, countries, program amounts, project titles, beneficiaries or participants, or stakeholders.

- External summary of no more than ten pages, which summarizes: the purpose of the evaluation; evaluation questions; evaluation design and methodology; and, findings. At the time of completion, the evaluation summary should be ready for publication to an external audience providing highlights from the evaluation report and may include a visual summary or infographic. This version of the report will be posted on the Department of State evaluation clearinghouse; thus, it should not include sensitive information or disclose the names of implementing partners, countries, project titles or amounts, beneficiaries or participants, or stakeholders.
- External fact sheet of concise findings: The fact sheet should be 1-2 pages and provide a concise summary of the findings of the evaluation. The fact sheet will be used externally and should not include sensitive information or disclose the names of implementing partners, countries, project titles or amounts, beneficiaries or participants, or stakeholders.

The overall evaluation should last no more than 12 months. The Contractor may wish to adjust the timetable, in consultation with and the approval of DRL.

Handover of Materials

Upon completion, all materials generated from this assignment—e.g. inception report, data collection instruments, field notes, analyzed and coded data which are anonymized, draft and final reports— shall be electronically packaged and delivered to DRL.

BUDGET

SOWs should be accompanied by a proposed budget for the evaluation. The estimate should cover items such as travel, team members' daily rates, interviewers and data processors, costs for printing, and other direct costs. There is no easy rule of thumb for estimating what an evaluation should cost. It depends on many factors, such as how broad or narrow the scope of the evaluation (that is, how many activities are included, how many evaluation questions are being asked), what evaluation methods have been selected, and the degree of validity (accuracy, reliability) being sought.

Person days can be budgeted by estimating the time required for (a) planning, (b) document review, (c) construction of research instruments, (d) data collection, (e) data analysis, (f) report writing, and (g) presentation.

The budget should be realistic and provision should be made for contingencies.

DRL EXPECTATIONS

- DRL will work with the Contractor to provide key information, documentation, and strategic guidance and to develop questions to be used in surveys, interviews, focus groups, or other evaluation methods. The Contractor will propose an initial evaluation design. The Contractor will work in consultation with DRL to shape the final evaluation design.
- The Contractor shall be responsive to DRL's needs throughout the project and demonstrate the ability to present information according to DRL's requests.
- At minimum, the Contractor shall hold weekly calls and provide a monthly written update (by the 10th day of each month, for the preceding month) to DRL, detailing the progress to date and explaining any

delays or challenges to maintaining the proposed work plan. The Contractor should also use these updates to identify any expectations for DRL, including requests for feedback, consultation or assistance with planning.

- The Contractor shall not contact any grantee organization or program partners in reference to this Statement of Work before the contract has been awarded, or without specific DRL permission.
- The Contractor shall provide all evaluation documentation (e.g., correspondence, contact letters, data collections instruments, reports, etc.) to DRL for review and clearance prior to disseminating to participants, key stakeholders, or any other evaluation subjects. Please provide two weeks for feedback periods. If urgent feedback is needed, please provide this notice as a written request.
- The Contractor shall forward all project deliverables to DRL in a timely manner, pending unforeseen delays. If extensions are needed, please provide this notice as a written request.
- DRL review of deliverables will focus on the quality of the deliverables and will relate to payments/invoicing regarding work completed.
- The Contractor and its in-country sub-contractors shall maintain the strict confidentiality of all data collected for this evaluation. The Contractor and its in-country sub-contractors shall assume primary responsibility for securing/verifying data that is collected. Security of this information is of the utmost importance given the sensitive nature of these projects. In addition, the contractor will detail its data retention policies, placing particular emphasis on how information gathered over the course of this contract will be used, transmitted, or stored during and upon completion of the contract.

PLACE OF PERFORMANCE

With the exception of data collection and briefings to DRL, project activity is anticipated to take place at the Contractor's place of work.

RESPONSIBILITY OF ALL COSTS

The Contractor shall assume responsibility for all costs associated with the project as detailed in the proposal. These costs include, but are not limited to: staff salaries; indirect costs; fee of any airfare and per diem for all contractor and sub-contractor staff domestic and international travel; security costs; securing and/or verifying contact information; data collection and data verification; lodging and per diem for interview or focus group participants (if necessary); lunch/dinner and incentive costs for interview and focus group participants; meeting room rentals for interviews and focus groups and other representational costs; telephone calls; mail and postage costs; and document reproduction.

NOTE: Contractors are asked to base the travel budget on economy class tickets. Contractors should not under-estimate the work time in foreign countries and the financial costs associated with overseas travel (i.e., per diem, security costs and airfare). All travel shall be in accordance with federal travel regulations, including "Preference for U.S.-Flag Air Carriers" (January 1997).

PERIOD OF PERFORMANCE

The period of performance for the evaluation shall not exceed 12 months.

ANNEX 2. EVALUATION METHODOLOGY

The evaluation team will conduct a mixed-method performance evaluation to answer the three EQs framing the IF Portfolio evaluation. The mixed-method evaluation design will integrate quantitative and qualitative data collection methods encompassing both primary and secondary data analysis. This approach will allow the evaluation team to present a comprehensive account of IF's results, including trends in strategies and best practices to address severe or emerging restrictions on freedom of expression and assembly or privacy online. In addition, the evaluation team will document useful lessons learned about the effectiveness of particular models or activities to inform future program design and evidence-based decision making.

To respond to the EQs, and as a best practice, DevTech has developed an **Evaluation Design Matrix,** Table 1, with a corresponding set of sub-EQs to help guide the evaluation design and analysis, to ensure that each of the four pillars and nine lines of effort are addressed, and that the resulting recommendations align with DRL/GP priorities and interests. The Evaluation Design Matrix presents the EQs and the proposed sub-EQs, and summarizes the data sources and analytical approaches that the evaluation team will draw on to respond to each EQ.

Table 1. Evaluation Design Matrix

Evaluation Question	Evaluation Sub-Question	Data Sources	Analytical Approaches
EQ.1. How effective are IF Programs completed within the last five years, as assessed against the IF Strategic Framework indicators, values, and goals?	1.a. To what extent, if any, and how has the IF Portfolio demonstrated progress against its established standard and custom indicators?	• Desk and Literature Review including IF program documentation as well as relevant academic and grey literature • Secondary Data Review of IF indicators and performance monitoring data as well as other relevant external indices • KIIs with DRL/GP Leadership and IF Portfolio Team Members • FGDs with Program Implementing Partners/Grantees	• Secondary Data Analysis • Thematic Analysis • Content Analysis
	1.b. To what extent, if any, and how has the IF Portfolio promoted the established values across each of the four pillars?	• Desk and Literature Review including IF program documentation as well as relevant academic and grey literature • Secondary Data Review of IF indicators and performance monitoring data as well as other relevant external indices • KIIs with DRL/GP Leadership and IF Portfolio Team Members • FGDs with Program Implementing Partners/Grantees	• Secondary Data Analysis • Thematic Analysis • Content Analysis
	1.c. To what extent, if any, and how has the IF Portfolio achieved the targeted goals for nine of the 14 lines of effort?	• Desk and Literature Review including IF program documentation as well as relevant academic and grey literature • Secondary Data Review of IF indicators and performance monitoring data as well as other relevant external indices • KIIs with DRL/GP Leadership and IF Portfolio Team Members • FGDs with Program Implementing Partners/Grantees	• Secondary Data Analysis • Thematic Analysis • Content Analysis
	1.d. To what extent, if any, and how has the IF Portfolio demonstrated alignment with other key DRL strategic policies and guidelines including the DOS Functional Bureau Strategies, National	• Desk and Literature Review including IF program documentation as well as relevant academic and grey literature	• Secondary Data Analysis • Thematic Analysis • Content Analysis

Evaluation Question	Evaluation Sub-Question	Data Sources	Analytical Approaches
	Security Strategy Guidance, and the National Cyber Strategy?	• Secondary Data Review of IF indicators and performance monitoring data as well as other relevant external indices • KIIs with DRL/GP Leadership and IF Portfolio Team Members • FGDs with Program Implementing Partners/Grantees	
EQ.2. How accurate are the assumptions that form the basis of the IF Strategic Framework Lines of Effort?	2.a. Anti-censorship Technology 2.b. Secure Communication 2c. DDOS Mitigation 2.d. Digital Security Capacity Building 2.e. Emergency Support 2.f. Public Awareness Raising and Education 2.g. Human Rights in Internet Policy 2.h. Legal Advocacy 2.i. Global Ranking	• Desk and Literature Review including IF program documentation as well as relevant academic and grey literature • KIIs with DRL/GP Leadership and IF Portfolio Team Members • FGDs with Program Implementing Partners/Grantees • Individual Subject-Matter Expert Discussions	• Contribution Analysis
EQ.3. 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?	3.a. Which safeguards have not been effective among these?	• Desk and Literature Review including IF program documentation as well as relevant academic and grey literature • Stock-taking Characterization Exercise: • Anonymous Online Survey • Follow-up Interviews • Case Studies • Expert Panel	• Characterization Analysis
	3.b. What are other effective safeguards that the DRL Internet Freedom team should consider utilizing to minimize IF-funded technologies for illicit purposes?	• Desk and Literature Review including IF program documentation as well as relevant academic and grey literature • Stock-taking Characterization Exercise: • Anonymous Online Survey • Follow-up Interviews • Case Studies • Expert Panel	• Characterization Analysis

The first two EQs are broad and macro-focused, designed to assess the progress of the IF portfolio collectively across each of the four pillars and nine lines of effort. EQs 1 and 2 will examine the effectiveness of the IF Portfolio and its program's related to technology development, digital safety, policy advocacy, and research. The third EQ, however, is specific and focused, and will be approached separately from EQs 1 and 2. EQ 3 is designed to increase DRL/GP's understanding of the success of current safeguards in minimizing the use of IF-funded technologies for illicit purposes under the technology development pillar.

While each EQ will draw on a unique set of data collection methods and tools, all three EQs will build upon a thorough desk and literature review. The evaluation team is conducting this review of the IF Portfolio and the program documentation provided by DRL/GP to gain an in-depth understanding of the IF Portfolio's activities and to assess the availability and quality of secondary data. As part of this process, the evaluation team will map the main documents and key partners and stakeholders to ensure that all the crucial elements are considered and analyzed. The following activities are planned as part of the desk review:

- Review the IF Strategic Framework and the corresponding objectives, values, and goals of IF, including those of each individual pillar, each line of effort, and each program. Specifically, at the program level, the evaluation team will review documentation pertinent to the 16 programs selected by DRL/GP to be targeted by the evaluation. These program-specific documents include, but are not limited to, available grant proposals, grant agreements, quarterly progress reports, final project reports, and project evaluations, focusing on the intervention logic, theory of change, and the results framework including indicators and benchmarks (baselines, targets, and sources of verification);
- Analyze progress and qualitative and quantitative monitoring reports;
- Review and analyze other reports produced by IF programs and provided to the evaluation team;
- Analyze products (reports and analyses) of other organizations, development partners, and academic institutions in the area of Internet freedom, human rights, and the flow and accessibility of online information, including products produced by other USG agents of change such as the DOS Bureau of Near Eastern Affairs (NEA), the US Agency for Global Media (USAGM), the Open Technology Fund (OTF), and the United States Agency for International Development (USAID), and identify possible best practices or lessons learned that could apply to future IF programming or strategy design;
- Analyze international practices and data from international indices relevant to the field of Internet freedom, human rights, and online information, where appropriate, collected and calculated by well-known, credible international think tanks and agencies (e.g., Research Project B, the Alliance for Affordable Internet, the International Telecommunications Union, the World Bank, and the Organization for Economic Cooperation and Development).

The desk review will continue throughout the evaluation, organizing information and evidence by EQ and sub-EQ to allow for structured data processing and analysis. To date, the desk review has helped inform the final EQs and sub-EQs, methodology, sampling, and draft data collection instruments. Following the submission of the draft desk and literature review, the evaluation team will submit the final data collection instruments to DRL/GP for review and approval prior to collecting primary data.

The following provides a detailed description of the proposed evaluation design and methodology for each of the three EQs. The discussion below includes justifications for the proposed approaches and an overview of the data collection methods and data analysis techniques we will employ, unique to each of the three EQs. We also provide an overview of our sampling plan across the identified key stakeholder groups.

EQ.1. How effective are IF Programs completed within the last five years, as assessed against the IF Strategic Framework indicators, values, and goals?

1.1. Approach

Evaluating effectiveness means that we will assess the stated goals and targeted outputs and outcomes of each line of effort to understand the extent to which they have been achieved. In addition, the evaluation team will examine the extent to which the programs have contributed to the indicators, values, and goals of the IF Strategic Framework. To respond to EQ 1, the evaluation team will draw on secondary data gathered from grantee program documents (e.g., program logic models, grant proposals, grant agreements, quarterly progress reports, final project reports, and individual project evaluations or internal reviews, as well as from DRL solicitations or Notices of Funding Opportunities) and end user utilization and feedback on IF-funded technologies from the IF program intermediaries. We will then analyze this data against indicators, goals, and values as stated in the IF Strategic Framework with specific relevance for each program. The evaluation team will also assess the program's alignment with other key DRL strategic policies and guidelines including the DOS Functional Bureau Strategies, National Security Strategy Guidance, and the National Cyber Strategy. To complement the evaluation's team review of secondary data and address any knowledge gaps, the evaluation team will conduct a series of semi-structured KIIs with DRL/GP Leadership and IF Portfolio team members and FGDs with program implementing partners or grantees for the 16 pre-selected programs.

Thus, to answer EQ 1, the evaluation team will employ an evaluation design that utilizes Secondary Analysis, Thematic Analysis, and Content Analysis. Secondary Analysis is a systematic research method that allows researchers to investigate secondary quantitative and qualitative sources to understand what is already known and what remains to be learned. Thematic and Content Analysis will be used to identify and categorize key themes, patterns, and trends to understand how IF staff and its implementing partners/grantees perceive the success of the portfolio. In some cases, this analysis will result in descriptive statistics that represent the level of goal achievement and therefore the effectiveness of programming.

1.2. Data Collection Methods and Tools

To answer EQ 1 and its corresponding sub-EQs, the evaluation team will use a mixed-method approach integrating qualitative and quantitative approaches to data collection. The following provides a detailed overview of the methods selected to inform EQ 1.

Desk and Literature Review. As described above, the initial stages of research consist of a combined desk and literature review. The evaluation team is studying the IF programming documentation and reports shared by DRL/GP as well as academic and gray literature to understand the context in which IF operates, challenges to Internet freedom, and global trends. This includes a review of the IF Portfolio's standard indicators, the values associated with each pillar, and the goals for each line of effort. In addition, the evaluation team is also reviewing program-level information to understand how the 16 pre-selected programs were designed to contribute to the overarching Strategic Framework as noted in, for example, the solicitations and grant awards, including an assessment of the individual theories of change and custom indicators. The desk and literature review also includes a review of existing indices on Internet freedom and related topics (e.g., digital transformation, open government, etc.) already collected and calculated by well-known, credible international think tanks and agencies (e.g., Research Project B, the Alliance for Affordable Internet, the International Telecommunications Union, the World Bank, and the Organization for Economic Cooperation and Development).

Secondary Data Review of IF Program Data and External Data. The evaluation team will review the IF Portfolio and program-level's available performance monitoring data, including the data related to both standard and custom indicators, as a starting point for assessing IF's effectiveness in achieving the defined indicators, values, and goals as outlined in IF's Strategic Framework. The evaluation team will also assess data quality and relevance to determine which data can be used to answer EQ 1, among others. Using independent data sources where appropriate and available, the evaluation team will provide an independent analysis of which indicator targets, values, and goals were met or significantly surpassed and begin identifying reasons behind any performance shortfalls. Through qualitative data collection, including KIIs and FGDs, the team will further explore spotlights of success as well as reasons for shortfalls.

Secondary Data Review of IF Program Intermediaries' Data. In addition to reviewing IF Program's available performance monitoring data, the evaluation team will engage with IF Program Intermediaries, the organizations using IF-funded technologies, to obtain existing data on the technologies end users' feedback and utilization. This data will allow the evaluation team to assess effectiveness of IF programming by understanding how the specific technology is being used, the frequency of use, and how the intended users have experienced the technology. Ultimately, this data should provide a glimpse into the impacts of the IF-funded technologies and whether the intended users have experienced greater access to information without rights-abusing surveillance or censorship and/or the ability to express their thoughts, opinions, and ideas without repercussion. The evaluation team does not intend to engage with end users directly but to collect anonymous data by extracting the data from the intermediaries' internal databases. The evaluation team will rely on the program implementing partners/grantees to request this information from their intermediaries.

Key Informant Interviews with DRL/GP Leadership and IF Portfolio Team Members. The DevTech evaluation team will conduct a series of KIIs with DRL/GP leadership and the IF team to inform EQ 1 by delving deeper into understanding the internal perceptions on the success of the IF Portfolio in achieving its established objectives, indicators, and values. The KIIs will also assess (1) DRL/GP perceptions of implementing partner/grantees' program implementation approaches; (2) the extent to which the activities addressed the key "problem areas" targeted in each line of effort's theory of change; and (3) capture lessons learned on what factors advanced success, what unintended outcomes may have occurred, and what constraints may have impeded progress.

The evaluation team will use a semi-structured approach to KIIs to ensure comparability, so that each interview will investigate the appropriate EQ and sub-EQs, while allowing some deviation given the diversity of programs implemented by the IF award. KIIs will be designed to last approximately 60 minutes. Drawing on a roster or organizational chart of the IF Portfolio team members to be provided by DRL/GP, the evaluation team will target senior team members from all nine levels of effort, past and present. These interviews will occur either in person, when possible, or online with the support of secure, password protected online call or video platforms (e.g., Teams or Zoom). Please refer to the sampling plan for additional details on the selection criteria and targeted respondent group.

Focus Group Discussions with Program Implementing Partners/Grantees. To inform EQ 1, the evaluation team will also facilitate a series of FGDs with the 16 pre-selected IF implementing partners/grantees. The evaluation team will rely on DRL/GP to introduce the evaluation team to the program's respective implementing partners/grantees. FGDs will be designed to (1) better understand and validate whether and where changes have occurred, whether intended or unintended, across each of the respective lines of effort; (2) what factors facilitated or hindered change; and (3) whether the changes observed are sustainable. FGDs will be conducted online using secure, password protected online call or video platforms as well as collaboration tools (e.g., Jamboard) across each of the nine lines of effort with the identified 16 programs. The evaluation team proposes to organize these FGDs by lines of effort to promote learning at the line of effort-level rather than at the individual program level. However, due to the sensitivity of the topics to be discussed, the evaluation team may decide, in collaboration with the grantees, to hold FGDs at the program level. The data generated from these FGDs will then be coded and analyzed at the line of effort-level, removing any and all personal identifiable information, and stored on a Virtual Private Network (VPN) protected site, accessible only to the core evaluation team. Please refer to the sampling plan for additional details on the selection criteria and targeted respondent group.

1.3. Design Validity and Triangulation

In addition to the methods and tools proposed above, the evaluation team reviewed a number of additional data collection methods and tools that could be used to generate useful findings in response to EQ 1, such as surveys and questionnaires and social network analysis. However, while all data collection methods and tools have strengths and weaknesses, the evaluation team determined that the EQ 1 findings and conclusions would be best achieved through secondary data review, KIIs, and FGDs.

Prior to data analysis, and to further validate the data collected through the proposed methods and tools, the evaluation team will triangulate the data continuously as data collection progresses to pursue new leads or verify contradictory information. Preliminary findings will be based on multiple sources of evidence, thereby increasing the strength, validity, and reliability of the evaluation's findings, conclusions and recommendations. The evaluation team will discuss preliminary findings during weekly evaluation team meetings throughout the data collection and analysis stage as well as with the evaluation's Contracting Officer's Representative (COR) during bi-weekly check-ins with the senior evaluator.

1.4. Data Analysis

To answer EQ 1, the evaluation team will first systematize the information produced during the desk review and data collection stages. Then, the evaluation team will analyze the data drawing on the systematic approach of Secondary Analysis combined with Thematic and Content Analysis, and adapt to this evaluation as follows:

- Identify the available sources of secondary data and assess its quality and relevance to EQ 1 and the respective sub-EQs.
- Conduct preliminary analysis of secondary data to understand whether and where change has occurred and document any knowledge gaps requiring further exploration through additional secondary data analysis or qualitative data collection. This preliminary analysis will inform the KII and FGD protocols and define the coding categories to support Thematic and Content Analysis.
- Following the completion of KIIs and FGDs, categorize and code qualitative data to assess the perceived levels of success of the IF Portfolio against the Strategic Framework. Using the interview and FGDs transcripts, produce case studies that speak to the objectives, goals, and values in the IF Strategic Framework.
- Triangulate across data sources to validate data, identify evidence-based findings, and produce conclusions describing the effectiveness of IF's current programming strategies, determining progress against the established outputs and outcomes, and develop action-oriented recommendations and lessons learned to strengthen future strategy design and program implementation to advance human rights.

EQ.2. How accurate are the assumptions that form the basis of the IF Strategic Framework Lines of Effort?

2.1. Approach

EQ 2 assesses the accuracy of the IF Portfolio's assumptions, which is to say, the foundational understanding of the different barriers to Internet freedom and the means to overcome them. IF restrictions are in place in diverse contexts that evolve over time. Any assessment of the accuracy of underlying assumptions must therefore consider the relative validity of such assumptions across space as well as the continued relevance of theories of change in the current context. Thus, the evaluation design calls for a theory-based approach, in which the accuracy and appropriateness of a program's theories of change are tested against evidence and, as needed, brought up to date. This theory-based approach will facilitate the application of this evaluation to program improvement decisions by not only gauging the relative accuracy of the underlying assumptions and theories of change against current conditions, but also describing the mechanisms by which the lines of effort were (or were not) effective in countering the many restrictions to Internet freedom in place across the IF Portfolio.

In light of such needs, to answer EQ 2, we will employ an evaluation design that inquires into the suitability of program design by looking not just at whether the assumptions still hold true, but also by updating these assumptions to match the observed reality by explaining why certain lines of effort were more effective in promoting Internet freedom than others. The "why" implies an understanding of cause-and-effect: which actions resulted in which outcomes in a particular setting. Contribution Analysis is an evaluation approach that complies with all such requirements.

Contribution Analysis is a theory-based approach used to evaluate programs in a complex and dynamic context. It aims to understand how the intervention contributes to (but cannot necessarily be attributed to) the achievement of certain outcomes, thereby demonstrating the value of the program and making decisions about its evolution or expansion. We will treat each line of effort as an intervention for the purpose of evaluating its contribution to the expected outcome, and therefore testing the accuracy of the assumptions behind it.

The approach consists of testing each line of effort's theory of change and the assumptions and hypotheses on which they are based. The goal is to formulate a reasonable and verified Contribution Story. To formulate this Contribution Story, the evaluation team will verify that:

- Each line of effort's theory of change is meaningful and clearly defined;
- That the line of effort's corresponding programs have been implemented as planned in its respective theory of change;
- That the theory of change is supported by evidence of observed results and underlying assumptions; and,
- Other factors that may influence the program's outcomes and underlying mechanisms were analyzed and found not to have had a significant impact or to have contributed to the outcomes achieved.

2.2. Data Collection Methods and Tools

To answer the EQ 2 and its corresponding sub-EQs, the evaluation team will draw primarily on qualitative approaches to data collection. The following provides a detailed overview of the methods selected to inform EQ 2.

Desk and Literature Review. The evaluation team will build upon the desk and literature review to study the programs further to determine assumptions present in the IF Portfolio strategic framework's lines of effort and related theories of change. The purpose of this analysis will be to (1) understand each line of effort's theory of change, including the mechanisms by which it is to bring about the intended transformations; (2) understand the influence of external factors and assumptions underlying each theory of change; (3) verify to what extent the theories of change are grounded in evidence (i.e., academic and grey literature) and are consistent with the latest documented practices of the lines of effort.

Semi-structured KIIs will be conducted with DRL/GP Leadership and the IF Portfolio's senior team members from all nine levels of effort, past and present. Interviews will be designed to cover topics responding to both EQs 1 and 2 and will last approximately 60 minutes. As noted above under EQ 1, team members will be identified using a roster or organizational chart of the IF Portfolio team members to be provided by DRL/GP. Please refer to the sampling plan for additional details on the selection criteria and targeted respondent group.

These interviews will produce insights concerning the status of each line of effort, its outcomes, any barriers that may be compromising the program's effectiveness, and challenges that may emerge in the future. During these interviews, the evaluators will also include open-ended questions about the existence of unexpected but observed outcomes. These unintended effects will be incorporated into the revised theories of change (see *Analysis* section below). Interviews will occur either in person, when possible, or online with the support of secure, password protected online call or video platforms (e.g., Teams or Zoom).

Focus group discussions (FGDs) will be held online with a secure, password protected online call or video platforms (e.g., Teams or Zoom) with the 16 pre-selected grantees following introductions facilitated by DRL/GP. Please refer to the sampling plan for additional details on the selection criteria and targeted respondent group. These FGDs will help the evaluation team to gather information concerning the IF Portfolio's effectiveness and the appropriateness of its assumptions. FGDs will also provide information concerning the programs developed, and the outcomes observed as a result of their actions. FGDs will be organized by lines of effort, responding to both EQs 1 and 2, to promote learning at the line of effort-level rather than at the individual program level. However, due to the sensitivity of the topics to be addressed, the evaluation team may decide, in collaboration with the grantees, to hold FGDs at the program level. The data generated from these FGDs will then be coded and analyzed at the line of effort-level, removing any and all personal identifiable information, and stored on a VPN-protected site, accessible only to the core evaluation team.

Individual discussions with independent subject-matter experts will take place online using a secure, password protected online call or video platforms (e.g., Teams or Zoom). The evaluation team has developed a list of SMEs based on a list of professional connections, notably those of our subject matter expert, Ms. Carolina Rossini. In collaboration with DRL/GP, the evaluation team will select a targeted respondent group with expertise corresponding to each of the nine lines of effort. Each interviewee will be presented in advance of the interview with the respective line of effort theory of change so they can reflect on its assumptions and provide deeper critical input about their likely effectiveness.

2.3. Design Validity and Triangulation

While the evaluation team explored numerous methods and tools to respond to EQ 2, such as path analysis and outcome mapping, the evaluation team determined that EQ 2 finding and conclusions would best be achieved by conducting individual semi-structured KIIs with senior IF Portfolio team members, FGDs with implementing partners/grantees, and individual discussions with independent subject-matter experts identified by the evaluation team's subject matter expert in consultation with DRL/GP.

Prior to data analysis, and to further validate the data collected through the proposed methods and tools, the evaluation team will triangulate the data continuously as data collection progresses to pursue new leads or verify contradictory information. Preliminary findings will be based on multiple sources of evidence, thereby increasing the strength, validity, and reliability of the evaluation's findings, conclusions and recommendations. The evaluation team will discuss preliminary findings during weekly evaluation team meetings throughout the data collection and analysis stage as well as with the evaluation's COR during bi-weekly check-ins with the senior evaluator.

2.4. Data Analysis

To answer EQ 2, we will systematize the information produced during the desk review and data collection stages and analyze it drawing from a procedure for Contribution Analysis suggested by Mayne (2001)[2], and adapted to this evaluation as follows:

- **Analyze the cause-effect relationship:** understand what outcomes the line of efforts is intended to achieve and how (by what mechanisms). We will develop a preliminary Contribution Story based on this analysis;
- **Assess the plausibility of alternative explanations:** check whether the desired results could have plausibly been generated by other mechanisms external to the program. This exercise will consist of studying historical, economic, and policy-specific factors related to obstacles to Internet freedom;
- **Re-assess the theories of change against evidence:** bring the theories of change up to date to match the line of efforts' assumptions against the observed needs, maximizing their effectiveness while retaining realistic expectations about their potential for effecting transformation; and
- **Formulate a Contribution Story:** produce a narrative of cause and effect and situate it in the realm of alternative causal explanations.

EQ.3. 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?

3.1. Approach

EQ 3 applies to programs within the Technology Pillar. It is a three-pronged question. It calls for the explanation of (1) *how* the safeguards laid out by DRL/GP have been successful in reducing the use of IF-funded technologies for illicit purposes, which presupposes that these safeguards were the "right" ones and to some extent successful, thus requiring that the evaluators identify safeguard success cases. This question also demands the identification of the coherence of the safeguards with the IF Strategic Framework. (2) The evaluation must also identify the safeguards that were not effective, if any. An identification exercise is likewise required to list and characterize them with respect to their ability or inability to meet the objectives of the IF Strategic Framework. (3) Finally, the evaluation must point to other measures that will likely decrease the likelihood that IF-funded technologies will be used for illicit purposes. In line with a previous study of illicit uses of IF-funded technologies commissioned by DRL/GP, we take "illicit use" or "illicit purposes" to

[2] Mayne J (2001) Addressing attribution through contribution analysis: using performance measures sensibly. Canadian Journal of Program Evaluation 16(1): 1–24.

be synonymous with criminal activity as defined U.S. or international law and/or that "reflect any type of support for any member, affiliate, or representative of a designated terrorist organization."[3][4].

To answer EQ 3 satisfactorily, the evaluation strategy must be both retrospective and prospective, looking at the achievements and limitations of the current safeguards and potentially proposing new, more effective ones. For the retrospective dimension, the evaluation team will conduct a stock-taking exercise of the existing IF Portfolio safeguards as defined in the FY2020 Department of State, Foreign Operations, and Related Programs (SFOPS) Appropriations Act and as implemented by the grantees of the Technology Pillar and characterize them. For the prospective dimension, the evaluation team will mobilize a panel of experts to discuss the findings of the stock-taking characterization exercise, potentially propose new safeguards – both technical and behavioral – and make suggestions to improve the existing ones.

3.2. Data Collection Methods and Tools

To answer the EQ 3 and its corresponding sub-EQs, the evaluation team will use a mixed-method approach integrating qualitative and quantitative approaches to data collection. The following provides a detailed overview of the methods selected to inform EQ 3.

Stock-taking characterization exercise. This stock-taking effort will be based on an *online anonymous survey* and *case studies* drafted from open-ended *follow-up voice interviews.*

- The **anonymous online survey** will request qualified informants from the implementing partner/grantees' staff to appraise the relative effectiveness of each safeguard they must put in place in accordance with DRL/GP guidelines to curb illicit use of the technology(ies) developed by their program. In another block of questions, the anonymous survey will ask about their awareness of instances where the technology in question could potentially be used for illicit purposes despite their best efforts. If the respondent agrees to be interviewed to further discuss the matter, s/he will be directed to a form hosted in a different server where s/he will provide contact information for a follow-up interview.
- The **follow-up interviews** with the implementing partner/grantees' qualified informant(s) will take place via a voice application with end-to-end cryptography such as Signal. After following the standard informed respondent consent protocol, the evaluator will gather detailed information about the effectiveness of the safeguards in place at that organizations utilizing the IF-funded technologies as verified by the implementing partner/grantee overseeing the program. The interviewer will prioritize a discussion of the safeguards that the respondent considered both particularly effective and ineffective in terms of their ability to deter or prevent illicit use.
- The anonymous data collected in the follow-up interviews will be stored on a VPN-protected site accessible only to the core evaluation team and will be triangulated with information from the document reviews where such safeguards are defined, to produce case studies describing how a given safeguard was observed to be especially effective or ineffective.
- A **case study** is a holistic, in-depth examination of a case (or cases) within its context. In program evaluations, case studies have different applications, but for our purposes it will serve an exploratory function: describing a phenomenon when not much –or nothing at all– is known about it. Our focus is

[3] Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva, Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals. Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR1151.html. Also available in print form.
[4] 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/

on producing a thorough description of the limitations or virtues of a given safeguard to be examined and commented upon by a panel of experts in the prospective stage that follows.

Expert Panel. The evaluation team will assemble a panel of subject matters experts specializing in the field of human rights safeguards that will meet online via a secure, password protected platform, to discuss a set of predetermined topics related to the vulnerability of safeguards to illicit use. The panel experts will be identified from the same pool of potential respondents as the independent SMEs described under EQ 2. The pool of potential informants was comprised based on the evaluation team's professional connections, notably those of our subject matter expert, Ms. Carolina Rossini. The evaluation team will select the panelist in collaboration with DRL/GP, ensuring that one expert does not participate in both the individual discussions and expert panels to ensure diverse points of view. Please refer to the sampling plan for additional details on the selection criteria and targeted respondent group.

Before the panel, these experts will be provided time-based, viewing only access to the anonymized case studies and the survey results on a secure, VPN-protected website. As part of the discussion, panelists will be invited to propose ways to improve the effectiveness of the existing safeguards and propose new ones based on their accumulated knowledge and individual research. The panel discussions will be transcribed, removing all personal identifiable information, and the recommendations drawn therein systematized as answers to items a) and b) of EQ 3.

3.3. Design Validity and Triangulation

To inform the evaluation design, the evaluation team reviewed a number of additional data collection methods and tools that could be used to generate useful findings in response to EQ 3, such as data scraping and observations. However, the evaluation team determined that EQ 3 findings and conclusions would best be achieved through a stock-taking characterization exercise and an expert panel.

Prior to data analysis, and to further validate the data collected through the proposed methods and tools, the evaluation team will triangulate the data continuously as data collection progresses to pursue new leads or verify contradictory information. Preliminary findings will be based on multiple sources of evidence, thereby increasing the strength, validity, and reliability of the evaluation's findings, conclusions and recommendations. The evaluation team will discuss preliminary findings during weekly evaluation team meetings throughout the data collection and analysis stage as well as with the evaluation's COR during bi-weekly check-ins with the senior evaluator.

3.4. Data Analysis

To answer EQ 3, the evaluation team will follow these analytic steps:

- **Preliminary analysis:** Identify the general and specific safeguards the IF Portfolio has in place in its programmatic strategy to prevent and mitigate illicit use of the technologies it supports. Then, identify the risks and benefits of those safeguards by means of the literature review. This preliminary analysis will inform the questions of the online survey as well as the follow-up interview guidelines.

- **Characterization:** Systematize the quantitative data from the survey to pinpoint which safeguarding measures are more and less effective and cross-tabulate them by type of technology, geographic area, relative risks, benefits, grantee and other variables of interest. Then, based on the follow-up interview transcriptions, produce unique case studies that speak to the objectives, goals, and values in the IF Portfolio's Strategic Framework. Answers to the general question in EQ 3, as well as to item a), will stem from this stage of the analysis.

- **Recommendations:** Systematize the joint analysis made by the safeguarding experts to produce actionable recommendations on potentially better measures to support IF safeguards, thus answering EQ 3 item b).

Sampling Plan

To answer the EQs in alignment with the proposed approaches, we propose the following purposive (i.e., non-random) sample of DRL/GP's IF Portfolio team members, implementing partners/grantees, independent SMEs, and a panel of outside experts. The sampling strategy is aimed at capturing a diversity of points of view. As in any qualitative research, the sample sizes are indicative and may be expanded if questions are not satisfactorily answered by the parties selected or reduced if responses show marginal or no new information.

4.1. KIIs with DRL/GP Leadership and IF Portfolio Team Members

The evaluation team will prepare a sample of DRL/GP Leadership and IF Portfolio team members to participate in KIIs as part of EQs 1 and 2. For each line of effort, we will interview senior staff at DRL/GP involved in its implementation of the IF Portfolio since its inception. If there are staff that have since left the program, we will contact those as well. Individual staff may be interviewed more than once if they are involved in more than one line of effort. Table 2 provides a list of proposed target respondents, with the final number of KIIs to be determined in collaboration with DRL/GP according to the availability of respondents and their relevance to the evaluation. The evaluation team will seek to ensure gender parity within the KIIs to the extent possible – however, the selection is primarily focused on the roles and responsibilities of key informants and their involvement in the project.

Table 2. KIIs Sampling

Stakeholder Type	Potential Respondent	Quantity
DRL/GP Leadership	Acting Principal Deputy Assistant Secretary	1
	Deputy Assistant Secretary	2
	Global Programming Director	1
	Global Programming Deputy Director	
DRL/GP IF Portfolio Team Members	Portfolio Manager	1
	Grant Manager	1
	Monitoring, Evaluation, and Learning (MEL) Specialist	1
	Line of Effort Manager/Technical Advisors	18 (2 per line of effort)
Total		**26**

4.2. FGDs with IF Grantees

To inform EQs 1 and 2, we will also conduct nine FGDs with implementing partners/grantees, one for each line of effort. Given COVID-19 restrictions and to elicit richer information during the discussions, FGDs will be conducted remotely and with four to six participants per group to allow for in-depth discussion in a remote format. To avoid domination by the more influential and eloquent participants, we will limit the discussion time for each FGD question and ensure all participants have a chance to answer the questions.

FGDs will include representatives from the pre-selected implementing partners/grantees associated with given line of effort (one or two grantees, depending on the line of effort). The FGDs will include representatives from different levels of the implementing partner/grantee's hierarchy, from management to staff. The implementing partners/grantees will be contacted directly from a sampling frame provided by DRL/GP (See Table 3). The evaluation team will engage with local researchers to conduct FGDs in the appropriate language, providing interpretation and translation support when needed. As noted above, however, due to the sensitivity of the topics to be addressed, the evaluation team may decide, in collaboration with the grantees, to hold FGDs at the program level. The data generated from these FGDs will then be coded and analyzed at the line of effort-level.

Table 3. FGDs Sampling

FGD	Pillar	Line of Effort	Grantee/s
1	Technology	Line of Effort 1: Anti-censorship Technology	Technology Project B Technology Project A
2	Technology	Line of Effort 2: Secure Communications	Technology Project C
3	Technology	Line of Effort 4: DDOS Mitigation	Technology Project D
4	Digital Safety	Line of Effort 6: Digital Security Capacity Building	Digital Safety Project A Digital Safety Project B
5	Digital Safety	Line of Effort 7: Emergency Support	Digital Safety Project C
6	Digital Safety	Line of Effort 8: Public Awareness Raising and Education	Digital Safety Project F Digital Safety Project E
7	Policy Advocacy	Line of Effort 9: Human Rights in Internet Policy	Policy Advocacy Project B Policy Advocacy Project A
8	Policy Advocacy	Line of Effort 12: Legal Advocacy	Policy Advocacy Project C Policy Advocacy Project D
9	Research	Line of Effort 13: Global Ranking	Research Project B Research Project A

4.3. Independent Subject Matter Experts

We will interview 18 subject-matter experts, two per line of effort to inform EQ 2, see Table 4. The experts will be selected from a pool of experts compiled by the evaluation team based on a list of professional connections and will be contacted directly by the evaluation team leader. The interviewees will be chosen, in consultation with DRL/GP, based on the affinity between their expertise and the subject of the level of effort at hand.

Table 4. Independent Subject Matter Experts Sampling

Stakeholder Type	Potential Respondent	Quantity
Subject Matter Experts	Internet Access and Anti-censorship Technology Specialist	2
	Online Surveillance and Secure Communications Specialist	2
	Countering Malign Online Attacks Specialist	2

Stakeholder Type	Potential Respondent	Quantity
	Digital Security Capacity Building Trainer/Specialist	2
	Digital Attacks and Emergency Support Specialist	2
	Public Awareness Raising Educator	2
	Human Rights Specialist	2
	Legal Advocate	2
	Internet Freedom Research Specialist	2
Total		**18**

4.4 Characterization Exercise

To inform EQ 3, the evaluation team will facilitate a characterization exercise drawing on an anonymous online survey, follow-up voice interviews, and featured case studies.

- The **anonymous online survey** will be sent out to the four pre-selected program's implementing partners/grantees in the Technology Pillar. The respondent of choice will be the most qualified person to answer questions about safeguards within the organization. If this information is not obvious from the available program documentation, it will be determined in consultation with the IF Portfolio team. There will be three reminder attempts to respondents that do not at first respond to the questionnaire.

- The **follow-up voice interviews** will be carried out with all respondents who noted on the survey that they agree to be interviewed using a voluntary response sampling approach.

- The quantity of featured **case studies** will depend on the number of valid answers to the survey and the diversity of situations emerging from the voice interviews. The evaluation team will strive to provide a balance of positive cases (success in using safeguards to minimize illicit use) and negative cases, in which the safeguards were insufficient to avoid illicit use to promote learning.

4.5 Expert Panel

The evaluation team will facilitate one expert panel to inform EQ 3 with approximately 3 – 5 participants, but no more than ten in total. The expert panelists will be selected from the evaluation team's network of contacts in the realm of human rights safeguards, in consultation with the DRL/GP IF team, and may be expanded upon using a snowball sampling approach[20] to reflect learning throughout the data collection process. Panelists will include representatives of academia, civil society, the US government, independent media outlets, the private sector, and/or philanthropic organizations.

ANNEX 3. DATA COLLECTION TOOLS

KII Introduction

Thank you for taking the time to talk to me. My name is [INSERT NAME]. With me, is my colleague [INSERT NAME], who will also participate in today's discussion by asking questions and taking notes. We are from DevTech Systems Inc., a U.S.-based international development advisory firm.

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 an evaluation of the Internet Freedom (IF) Portfolio. The purpose of the evaluation is to (1) examine the effectiveness of IF's overarching strategy and current programming in meeting its established objectives and goals; (2) garner important implementation lessons learned that can be applied to future programming; (3) assess progress at the output and outcome levels; and (4) ascertain any unintended outcomes, whether positive or negative, resulting from programming.

I would like to ask you questions related to your expertise and experience with Internet Freedom.

This interview will last approximately one hour (1h). With your permission, I would like to audio record this session for report writing and analysis purposes only. The recordings will be destroyed once we complete our analysis. Is this okay with you?

□ Yes

□ No

In the evaluation report, your name will not be mentioned. The evaluation team will make every effort to protect the anonymity and confidentiality of our discussion and hope you will feel comfortable providing honest feedback on your experiences and points of view. Participation is voluntary; also, you may decline to respond to our questions or end the interview at any time. Do you have any questions?

Can we start now?

□ Yes

□ No

DRL/GP LEADERSHIP KII GUIDE

Interview Information	
Date	
Interviewer Name	
Primary Notetaker Name	

Respondent Information	
Respondent Name	
Respondent Organization	
Respondent Title	
Stakeholder Type	□ DRL/GP Leadership □ Internet Freedom Portfolio Team Member □ Subject-Matter Expert □ Academic □ Business Representative □ Civil Society Representative □ Technical Expert □ Government Expert □ Other Donor □ Other - _______________
Gender	□ Male □ Female □ Other □ Refusal

1. Please tell me a bit about your role on the Internet Freedom Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Can you describe your level of engagement, if any, with the IF Portfolio team? The program implementing partners/grantees?

3. How would you define the success of the IF Portfolio?

   - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

   - Were there any results or outcomes that surprised you, either positively or negatively?

4. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

5. Based on your observed experience, to what extent has the IF Portfolio contributed to providing and/or enhancing access to the global Internet? Please explain.

   - Can you provide an example?

- Were there any barriers or challenges that the Portfolio encountered which may have impeded its effectiveness in connecting individuals and communities to the internet?

6. Based on your observed experience, to what extent has the IF Portfolio enhanced digital security training and capacity building for activities that support democratic processes/values? Combating violence against bloggers and other users? Please explain.

    - Can you provide an example?

    - Were there any barriers or challenges that the Portfolio encountered which may have impeded its effectiveness in delivering training and building stakeholders capacity?

7. Based on your observed experience, to what extent has the IF Portfolio supported efforts to counter the development of repressive Internet related laws and regulations? Please explain.

    - Can you provide an example?

    - Were there any barriers or challenges that the Portfolio encountered which may have impeded its effectiveness in addressing repressive Internet related laws and regulations?

8. Based on your observed experience, to what extent has the IF Portfolio contributed to expanding available research and evidence related to key threats to Internet Freedom? Please explain.

    - Can you provide an example?

    - Were there any barriers or challenges that the Portfolio encountered which may have impeded its effectiveness in expanding the knowledge base on key threats to Internet Freedom?

9. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

10. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IF PORTFOLIO TEAM MEMBER FACILITATION GUIDE

Interview Information	
Date	
Interviewer Name	
Primary Notetaker Name	

Respondent Information	
Respondent Name(s)	
Respondent Organization	
Respondent Title(s)	
Stakeholder Type	□ DRL/GP Leadership □ Internet Freedom Portfolio Team Member □ Subject-Matter Expert □ Academic □ Business Representative □ Civil Society Representative □ Technical Expert □ Government Expert □ Other Donor □ Other - ________________
Gender(s)	□ Male □ Female □ Other □ Refusal

General Questions

1. Please tell me a bit about your role on the Internet Freedom Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would you define the success of the IF Portfolio?

    - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

    - Were there any results or outcomes that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the program implementing partners/grantees?

Pillar No. 1: Technology, Part 1

Line of Effort #1, Anti-Censorship Technology

1. Based on your observed experience, how does technology help exercise Internet freedom? Can technology help to overcome restrictions?

2. Based on your observed experience with the programs under the IF Portfolio, do you feel that anti-censorship technologies help bypass censorship? If yes, can you please provide an example? If not, why do you feel that way?

3. Based on your observed experience, are anti-censorship technologies enough to circumvent Internet blockages and provide safe, reliable, and secure access to the Internet in repressive contexts? If not, what else is necessary?

4. Based on your observed experience, what limitations have you observed in the anti-censorship technologies currently available? Do you have any recommendations for future anti-censorship programming/grant making?

5. Based on your observed experience, do anti-censorship technologies allow for the online exercise of human rights and fundamental freedoms? Please explain.

   - In your opinion, do some technologies support one human right more fully than another?

6. Based on your observed experiences, what are the most helpful and the least helpful anti-censorship technologies to bypass censorship and improve access to the open Internet? (e.g., proxies and VPNs, pluggable transports, network obfuscation and anonymity, refraction routing, domain fronting, content delivery networks, white label apps)

7. Based on your observed experience, can anti-censorship technologies be used—or are they being used—for illicit activities? Are there ways to minimize their use for illicit purposes?

   - Is there evidence that any specific anti-censorship technology is optimized for illicit purposes? Please explain.

   - Is there evidence that specific illicit activity is only possible with the capabilities of the DRL-funded anti-censorship technology? Please explain.

Line of Effort #2, Secure Communications

8. In oppressive societies, is secure communications essential to protect one's privacy? Please explain.

9. Based on your observed experience, to what extent have IF programs contributed to providing a means to protect communications in surveilled environments or environments where privacy is not protected or is threatened? Please explain.

10. Based on your observed experience, to what extent can technology provide a means to protect communications in surveilled environments where privacy is not protected or is threatened?

11. Based on your observed experience, how are the following technologies helpful or not helpful for users to achieve surveillance-free communications and protect their privacy?
    - Secure file transfer

    - Encrypted chat

    - Anonymous and obfuscated communication protocols

    - White label apps

12. Based on your observed experience, what approaches have you found to be effective to achieve surveillance-free communications and protect privacy within DRL's targeted communities?

13. Based on your observed experience, what are the socio-economic barriers to the adoption and utilization of DRL-funded technologies/activities? What are the technical barriers to the adoption and utilization of DRL-funded technologies/activities?

14. Based on your observed experience, what other factors or characteristics are important to secure communications in terms of technology and the Internet?

15. Based on your observed experience, are secure communications technologies used—or can they be used—for illicit activities? Are there ways to minimize their use for illicit purposes?

    - Is there evidence that any specific secure communications technology is optimized for illicit purposes? Please explain.

    - Is there evidence that specific illicit activity is only possible with the capabilities of the DRL-funded secure communications technology? Please explain.

Pillar No. 1: Technology, Part 2

Line of Effort #4, DDOS Mitigation

1. Based on your observed experience, to what extent have IF programs helped with website protection from DDOS attacks? Please explain.

2. What has been your experience with DDOS as an attack weapon to stifle expression? How does it rank with other means used by state and non-state actors to stifle expression?

3. Based on your observed experience, can DDOS mitigation platforms protect websites/organizations/individuals? Please explain.

4. Based on your observed experience, what are the most helpful and the least helpful approaches to DDOS attack mitigation? What else is out there? What else should DRL consider funding?

    - Free protection services for vulnerable civil society and media groups?
    - Website mirroring?
    - Botnet attack forensics and attribution?
    - Threat intelligence and sharing?

5. Based on your observed experience, what are the socio-economic barriers to the adoption and utilization of DRL-funded technologies/activities? What are the technical barriers to the adoption and utilization of DRL-funded technologies/activities?

6. Based on your observed experience, are DDoS mitigation solutions and secure hosting technologies used for—or can they be used for—illicit activities? Are there ways to minimize their use for illicit purposes?

   - Is there evidence that any specific DDoS mitigation solutions and secure hosting technology is optimized for illicit purposes? Please explain.

   - Is there evidence that specific illicit activity is only possible with the capabilities of the DRL-funded DDoS mitigation solutions and secure hosting technology? Please explain.

Safeguards

7. Based on your observed experience, what safeguards are effective—and what are ineffective—to minimize the use of technology for illicit activities? Why?

   - Is there evidence that any specific safeguards are efficient in minimizing the use of DRL-funded technologies for illicit purposes? Please explain.

8. Based on your observed experience, what safeguards, if any, would fundamentally compromise the utility of DRL-funded technologies for their intended purposes of allowing for the online exercise of human rights and fundamental freedoms?

9. Based on your observed experience, are there any types of safeguards which, if implemented, would be used to support efforts to actively INFRINGE on the exercise of human rights and fundamental freedoms?

10. Based on your observed experience, what types of safeguards against the illicit use of DRL-funded technologies are the most effective? The least effective? Why?

   - (a) human based safeguards (e.g., behavioral, partnership, vetting, targeted community building campaigns, education, etc.)
   - (b) technology-based safeguards (e.g., audit control, integrity control, open source, backdoors and master keys, etc.)
   - (c) principle-based safeguards (e.g., human rights by design, etc.)

11. Based on your observed experience, are there additional safeguards to minimize illicit activity via these technologies not previously mentioned that would be effective? Please explain.

12. Based on your observed experience, are there additional safeguards which are commonly recommended as ways to minimize illicit activity that are ineffective at minimizing illicit activity?

13. Based on your observed experience, are there additional safeguards which are commonly recommended as ways to minimize illicit activity that would be actively detrimental to the ability of these technologies to carry out their intended purposes of allowing for the online exercise of human rights and fundamental freedoms?

Pillar No. 2: Digital Safety

Line of Effort #6, Digital Security Capacity Building

1. Based on your observed experience, to what extent have IF programs contributed to civil society's work by deterring digital threats? Please explain.

2. Based on your observed experience, have the following activities contributed to a stronger proactive digital security capacity for civil society and human rights defenders? Which are the most effective? What other activities are possible?

   - Targeted training?
   - Risk assessment and mitigation planning?
   - Organizational security auditing?
   - Systemic approach to digital safety in civil society and human rights organizations?
   - Digital security-sharing and coordination with civil society networks?
   - Other?

3. Based on your observed experience, what are the socio-economic barriers to the adoption and utilization of DRL-funded technologies/activities? What are the technical barriers to the adoption and utilization of DRL-funded technologies/activities?

4. Based on your observed experience, in adverse circumstances, are the following digital safety capacities critical for safe operations: skill setting, staffing and leadership, organizational structure and systems? What else is possible?

Line of Effort #7, Emergency Support

5. Based on your observed experience, to what extent have IF programs contributed to the mitigation of damages caused by digital attacks? Please explain.

6. Based on your observed experience, what types of emergency support are most effective (examples below)? What else could be made available?

   - Helplines?
   - Post-incident response mediations?
   - Open-source threat forensics, research analysis, and prediction?
   - Global threat-sharing and coordination with civil society networks?

7. Based on your observed experience, what are the socio-economic barriers to the adoption and utilization of DRL-funded technologies/activities? What are the technical barriers to the adoption and utilization of DRL-funded technologies/activities?

8. Based on your observed experience, do you believe that a disruption to the work of civil society can have a negative impact on the expansion of democratic values and the protection of human rights? Please explain.

9. Based on your observed experience, is emergency support effective for reducing the impacts of digital attacks? What else is important to reduce the impacts of digital attacks?

Line of Effort #8, Public Awareness Raising and Education

10. Based on your observed experience, to what extent have IF programs contributed to a better understanding of digital security risks among civil society and the public at large? Please explain.

11. Based on your observed experience, to what extent have IF programs contributed to improving and scaling educational support services to increase one's awareness of the potential digital security risks facing civil society and the public at large?

12. Based on your observed experience, which of the following methods of public awareness raising and education are available to civil society and the public at large and effective for improving their understanding of the existing and emerging digital security risks they may encounter?

    - Individual resources?
    - Localized educational resources?
    - Adult education methodologies promoting digital literacy?
    - Global online training platforms?
    - Curriculum design and standard setting?
    - Campaigns?

13. Based on your observed experience, what are the socio-economic and technical barriers to the adoption of better digital security by organizations and the public at large?

14. Based on your observed experience, is digital literacy essential for digital security education? What else is important in order to develop digital security education?

15. Based on your observed experience, why are tailored resources important to civil society and marginalized populations? What else is important to support these groups specifically?

Pillar No. 3: Political Advocacy and Pillar No. 4: Research

Line of Effort #9, Human Rights in Internet Policy

1. Based on your observed experience, to what extent have IF programs provided human rights defenders access to advocate for human rights in multi-stakeholder technology policy and standards fora? Please explain.

2. Based on your observed experience, to what extent have IF programs strengthened the capacity of human rights defenders to advocate for human rights in multi-stakeholder technology policy and standards fora? Please explain.

3. Based on your observed experience, to what extent have the DRL-assisted civil society organizations successfully advocated for the protection of human rights online?

   - In what type of fora (local, national, regional, global) have DRL-assisted civil society organizations been more effective in advocating for the protection of human rights online?

4. Based on your observed experience, what types of engagements with other stakeholders help or hurt civil society advocacy for human rights online?

5. Based on your observed experience, do DRL-assisted civil society organizations lack knowledge, access, or capacity to engage in standards-setting? In what circumstances? What areas of assistance do DRL-assisted civil society organizations generally need support in?

6. Based on your experience, in the context of Internet policy development, is a multi-stakeholder approach important to ensure the Internet is rights-respecting? Why? What else is important?

Line of Effort #12, Legal Advocacy

7. Based on your observed experience, to what extent have IF programs contributed to a greater respect for rule of law that ensures protections of human rights online? Please explain. Can you provide an example or two?

8. Based on your observed experience, have you found that the role of strategic litigation can help the exercise of human rights on the Internet? If yes, how? If no, why?

9. Based on your observed experience, have you found that training law practitioners and judges can help the exercise of human rights on the Internet? If yes, how? If no, why?

10. Based on your observed experience, are legal challenges effective to address repressive application of the judiciary and law enforcement to restrict human rights online in countries with rule of law? If yes, how? If no, why not?

11. Based on your observed experience, what is the effectiveness of organizations lobbying in congress for changes and/or improvements within the legal and regulatory environment?

Line of Effort #13, Global Rankings

12. Based on your observed experience, what legal and policy analyses and/or relevant metrics exist to support civil society and human rights defenders in effectively comparing laws, policies, and procedures that respect human rights online across countries and regions?

13. Based on your observed experience, what approaches do civil society and human rights defenders use to measure how laws, policies, and procedures respect human rights online? Are these approaches effective? Why or why not?

14. Based on your observed experience, to what extent have IF programs contributed to creating an objective and comparable metric for laws, policies, and procedures that respect human rights online? Please explain.

15. Based on your observed experience, are the legal and policy analyses currently available accurate and applicable research to ensure the respect and protection of human rights online?

16. What are the biggest challenges and barriers to ensuring civil society and human right defenders can measure laws, policies, and procedures and the extent to which they respect and protect human rights online?

17. What are the known or emerging issues that should be considered when designing metrics to measure the aforementioned laws, policies, and procedures?

Looking Ahead

18. Based on your experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

Focus Group Discussion Introduction and Sign-In Sheet

Evaluation of the Internet Freedom Portfolio Activities

Thank you for taking the time to participate in this focus group discussion. My name is [INSERT NAME]. With me, is my colleague [INSERT NAME], who will also participate in today's discussion by asking questions and taking notes. We are from DevTech Systems Inc., a U.S.-based international development advisory firm.

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 an evaluation of the Internet Freedom (IF) Portfolio. The purpose of the evaluation is to (1) examine the effectiveness of IF's overarching strategy and current programming in meeting its established objectives and goals; (2) garner important implementation lessons learned that can be applied to future programming; (3) assess progress at the output and outcome levels; and (4) ascertain any unintended outcomes, whether positive or negative, resulting from programming. Through this focus group discussion, we hope to learn about your experiences with the IF Portfolio, including why activities were effective or ineffective, the challenges you experienced (if any), as well as the outcomes of your collaboration with these activities.

This discussion will last approximately 90 minutes. With your permission, I would like to audio record this session for report writing and analysis purposes only. The recordings will be destroyed once we complete our analysis. Is this okay with each of you?

□ Yes

□ No

In the evaluation report, your names will not be mentioned. The evaluation team will make every effort to protect the anonymity and confidentiality of our discussion and hope you will feel comfortable providing honest feedback on your experiences and points of view. Participation is voluntary; also, you may decline to respond to our questions or end the interview at any time. Do you have any questions?

Can we start now?

□ Yes

□ No

Informed Consent: The FGD facilitator will explain the purpose of the meeting and administer the informed consent protocol (which includes information about IF, the purpose of evaluation, and explains that their participation is voluntary, and that information shared will be kept confidential). The facilitator will also request that participants in the group respect the confidentiality of their co-participants by not discussing what was discussed with others outside the group.

Data Security: The FGD facilitator will provide an overview of the team's data security protocols and review these at the start of the meeting.

Introductions: We will ask each participant to introduce herself/himself and briefly his/her role on the IF Project in discussion. Pending participants consent, the FGD facilitator will begin recording the discussion for data analysis purposes following introductions.

Sign-in Sheet: At the start of the discussion, participants will be prompted to complete a questionnaire to provide their name, title, organization, and gender. It will be explained that this written information will only be available to the facilitators and that the discussion will happen under Chatham House rules.

Facilitator Information	
Date	
Facilitator Name	
Primary Notetaker Name	
Relevant Pillar(s)	□ Technology □ Digital Safety □ Policy Advocacy □ Research
Relevant Line(s) of Effort	□ Line of Effort 1: Anti-Censorship Technology □ Line of Effort 2: Secure Communications □ Line of Effort 4: DDoS Mitigation □ Line of Effort 6: Digital Security Capacity Building □ Line of Effort 7: Emergency Support □ Line of Effort 8: Public Awareness Raising and Education □ Line of Effort 9: Human Rights in Internet Policy □ Line of Effort 12: Legal Advocacy □ Line of Effort 13: Global Ranking

Participant Information					
Name	Title	Organization	Program/Grant	Country of Origin	Sex
					□ Male □ Female □ Other □ Refusal
					□ Male □ Female □ Other □ Refusal
					□ Male □ Female □ Other □ Refusal
					□ Male □ Female □ Other □ Refusal
					□ Male □ Female □ Other □ Refusal
					□ Male □ Female □ Other □ Refusal
					□ Male □ Female □ Other □ Refusal
					□ Male □ Female □ Other □ Refusal

IMPLEMENTING PARTNER, LOE NO. 1, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your organization's program?

   - Did the program develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?

   - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

   - Were there any results or outcomes from your program that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #1, Anti-Censorship Technology

5. Based on your observed experience, to what extent has your organization's program contributed to increasing access to the global Internet? Please explain.

6. Based on your observed experience, how does technology help exercise Internet freedom? Can technology help to overcome restrictions?

7. Based on your observed experience with your organization's program, do you feel that anti-censorship technologies help bypass censorship? If yes, can you please provide an example? If not, why do you feel that way?

8. Based on your observed experience, are anti-censorship technologies enough to circumvent Internet blockages and provide safe, reliable, and secure access to the Internet in repressive contexts? If not, what else is necessary?

9. Based on your observed experience, what limitations have you observed in the anti-censorship technologies currently available? Do you have any recommendations for future anti-censorship programming/grant making?

10. Based on your observed experience, do anti-censorship technologies allow for the online exercise of human rights and fundamental freedoms? Please explain.

    - In your opinion, do some technologies support one human right more fully than another?

11. Based on your observed experiences, what are the most helpful and the least helpful anti-censorship technologies to bypass censorship and improve access to the open Internet? (e.g., proxies and VPNs, pluggable transports, network obfuscation and anonymity, refraction routing, domain fronting, content delivery networks, white label apps)

12. Based on your observed experience, are anti-censorship technologies used—or can they be used—for illicit activities? Are there ways to minimize their use for illicit purposes?

    - Is there evidence that any specific anti-censorship technology is optimized for illicit purposes? Please explain.

    - Is there evidence that specific illicit activity is only possible with the capabilities of the DRL-funded anti-censorship technology? Please explain.

13. Based on your observed experience, what safeguards are effective—and ineffective—ways to minimize the use of anti-censorship technology for illicit activities? Why?

    - Is there evidence that any specific safeguards are efficient in minimizing the use of DRL-funded anti-censorship technologies for illicit purposes? Please explain.

14. Based on your observed experience, what safeguards, if any, would fundamentally compromise the utility of these anti-censorship technologies for their intended purposes of allowing for the online exercise of human rights and fundamental freedoms?

15. Based on your observed experience, are there any types of safeguards which, if implemented, would be used to support efforts to actively INFRINGE on the exercise of human rights and fundamental freedoms?

16. Based on your observed experience, what types of safeguards against the illicit use of DRL-funded anti-censorship technologies are the most effective? The least effective? Why?

    - (a) human based safeguards (e.g., behavioral, partnership, vetting, targeted community building campaigns, education, etc.)
    - (b) technology-based safeguards (e.g., audit control, integrity control, open source, backdoors and master keys, etc.)
    - (c) principle-based safeguards (e.g., human rights by design, etc.)

17. Based on your observed experience, are there additional safeguards to minimize illicit activity via anti-censorship technologies not previously mentioned that would be effective? Please explain.

18. Based on your observed experience, are there additional safeguards which are commonly recommended as ways to minimize illicit activity that are ineffective at minimizing illicit activity?

19. Based on your observed experience, are there additional safeguards which are commonly recommended as ways to minimize illicit activity that would be actively detrimental to the ability of these anti-censorship

technologies to carry out their intended purposes of allowing for the online exercise of human rights and fundamental freedoms?

Looking Ahead

20. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

21. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IMPLEMENTING PARTNER, LOE NO. 2, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your program?

   - Did the program develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?

   - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

   - Were there any results or outcomes from your program that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #2, Secure Communications

5. Based on your observed experience, in oppressive societies, is secure communications essential to protect one's privacy? Please explain.

6. Based on your observed experience, to what extent has your organization's program contributed to providing a means to protect communications in surveilled environments or environments where privacy is not protected or is threatened? Please explain.

7. Based on your observed experience, to what extent can technology provide a means to protect communications in surveilled environments where privacy is not protected or is threatened?

8. Based on your observed experience, how are the following technologies helpful or not helpful for users to achieve surveillance-free communications and to best protect their privacy?

   - Secure file transfer

   - Encrypted chat

   - Anonymous and obfuscated communication protocols

- White label apps

9. Based on your observed experience, what approaches have you found to be effective to achieve surveillance-free communications and protect privacy within DRL's targeted communities?

10. Based on your observed experience, what are the socio-economic barriers to the adoption and utilization of DRL-funded technologies/activities? What are the technical barriers to the adoption and utilization of DRL-funded technologies/activities?

11. Based on your observed experience, what other factors or characteristics are important to secure communications in terms of technology and the Internet?

12. Based on your observed experience, are secure communications technologies used—or can they be used—for illicit activities? Are there ways to minimize their use for illicit purposes?

    - Is there evidence that any specific secure communications technology is optimized for illicit purposes? Please explain.

    - Is there evidence that specific illicit activity is only possible with the capabilities of the DRL-funded secure communications technology? Please explain.

13. Based on your observed experience, what safeguards are effective—and ineffective—ways to minimize the use of secure communications technology for illicit activities? Why?

    - Is there evidence that any specific safeguards are efficient in minimizing the use of DRL-funded secure communications technologies for illicit purposes? Please explain.

14. Based on your observed experience, what safeguards, if any, would fundamentally compromise the utility of these secure communications technologies for their intended purposes of allowing for the online exercise of human rights and fundamental freedoms?

15. Based on your observed experience, are there any types of safeguards which, if implemented, would be used to support efforts to actively INFRINGE on the exercise of human rights and fundamental freedoms?

16. Based on your observed experience, what types of safeguards against the illicit use of DRL-funded secure communications technologies are the most effective? The least effective? Why?

    - (a) human based safeguards (e.g., behavioral, partnership, vetting, targeted community building campaigns, education, etc.)
    - (b) technology-based safeguards (e.g., audit control, integrity control, open source, backdoors and master keys, etc.)
    - (c) principle-based safeguards (e.g., human rights by design, etc.)

17. Based on your observed experience, are there additional safeguards to minimize illicit activity via secure communications technologies not previously mentioned that would be effective? Please explain.

18. Based on your observed experience, are there additional safeguards which are commonly recommended as ways to minimize illicit activity that are ineffective at minimizing illicit activity?

19. Based on your observed experience, are there additional safeguards which are commonly recommended as ways to minimize illicit activity that would be actively detrimental to the ability of these secure communications technologies to carry out their intended purposes of allowing for the online exercise of human rights and fundamental freedoms?

Looking Ahead

20. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

21. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IMPLEMENTING PARTNER, LOE NO. 4, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your program?

   - Did you develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?

   - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

   - Were there any results or outcomes that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #4, DDOS Mitigation

5. Based on your observed experience, to what extent has your organization's program helped with website protection from DDOS attacks? Please explain.

6. Based on your observed experience, what has been your experience with DDOS as an attack weapon to stifle expression? How does it rank with other means used by state and non-state actors to stifle expression?

7. Based on your observed experience, can DDOS mitigation platforms protect websites/organizations/individuals? Please explain.

8. Based on your observed experience, what are the most helpful and the least helpful approaches to DDOS attack mitigation? What else is out there? What else should DRL consider funding?
   - Free protection services for vulnerable civil society and media groups?
   - Website mirroring?
   - Botnet attack forensics and attribution?
   - Threat intelligence and sharing?

9. Based on your observed experience, what are the socio-economic barriers to the adoption and utilization of DRL-funded technologies/activities? What are the technical barriers to the adoption and utilization of DRL-funded technologies/activities?

10. Based on your observed experience, are DDoS mitigation solutions and secure hosting technologies used for—or can they be used for—illicit activities? Are there ways to minimize their use for illicit purposes?

    - Is there evidence that any specific DDoS mitigation solutions and secure hosting technology is optimized for illicit purposes? Please explain.

    - Is there evidence that specific illicit activity is only possible with the capabilities of the DRL-funded DDoS mitigation solutions and secure hosting technology? Please explain.

11. Based on your observed experience, what safeguards are effective—and ineffective—ways to minimize the use of DDoS mitigation solutions and secure hosting technology for illicit activities? Why?

    - Is there evidence that any specific safeguards are efficient in minimizing the use of DRL-funded DDoS mitigation solutions and secure hosting technologies for illicit purposes? Please explain.

12. Based on your observed experience, what safeguards, if any, would fundamentally compromise the utility of these DDoS mitigation solutions and secure hosting technologies for their intended purposes of allowing for the online exercise of human rights and fundamental freedoms?

13. Based on your observed experience are there any types of safeguards which, if implemented, would be used to support efforts to actively INFRINGE on the exercise of human rights and fundamental freedoms?

14. Based on your observed experience, what types of safeguards against the illicit use of DRL-funded DDoS mitigation solutions and secure hosting technologies are the most effective? The least effective? Why?

    - (a) human based safeguards (e.g., behavioral, partnership, vetting, targeted community building campaigns, education, etc.)
    - (b) technology-based safeguards (e.g., audit control, integrity control, open source, backdoors and master keys, etc.)
    - (c) principle-based safeguards (e.g., human rights by design, etc.)

15. Based on your observed experience, are there additional safeguards to minimize illicit activity via DDoS mitigation solutions and secure hosting technologies not previously mentioned that would be effective? Please explain.

16. Based on your observed experience, are there additional safeguards which are commonly recommended as ways to minimize illicit activity that are ineffective at minimizing illicit activity?

17. Based on your observed experience, are there additional safeguards which are commonly recommended as ways to minimize illicit activity that would be actively detrimental to the ability of these DDoS mitigation solutions and secure hosting technologies to carry out their intended purposes of allowing for the online exercise of human rights and fundamental freedoms?

Looking Ahead

18. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

19. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IMPLEMENTING PARTNER, LOE NO. 6, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your program?

   - Did you develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?
   - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?
   - Were there any results or outcomes that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #6, Digital Security Capacity Building

5. Based on your observed experience, to what extent has your organization's program contributed to civil society's work by deterring digital threats? Please explain.

6. Based on your observed experience, have the following activities contributed to a stronger proactive digital security capacity for civil society and human rights defenders? Which are the most effective? What other activities are possible?
   - Targeted training?
   - Risk assessment and mitigation planning?
   - Organizational security auditing?
   - Systemic approach to digital safety in civil society and human rights organizations?
   - Digital security-sharing and coordination with civil society networks?
   - Other?

7. Based on your observed experience, what are the socio-economic barriers to the adoption and utilization of DRL-funded technologies/activities? What are the technical barriers to the adoption and utilization of DRL-funded technologies/activities?

8. Based on your observed experience, in adverse circumstances, how, if at all, are the following digital safety capacities critical for safe operations: skill setting, staffing and leadership, organizational structure and systems? What other capacities not already mentioned are critical?

Looking Ahead

9. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

10. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IMPLEMENTING PARTNER, LOE NO. 7, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your program?

    - Did you develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?

    - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

    - Were there any results or outcomes that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #7, Emergency Support

5. Based on your observed experience, to what extent has your organization's program contributed to the mitigation of damages caused by digital attacks? If yes, how much? Please explain.

6. Based on your observed experience, what types of emergency support are most effective (examples below)? What else could be made available?

    - Helplines?
    - Post-incident response mediations?
    - Open-source threat forensics, research analysis, and prediction?
    - Global threat-sharing and coordination with civil society networks?

7. Based on your observed experience, what are the socio-economic barriers to the adoption and utilization of DRL-funded technologies/activities? What are the technical barriers to the adoption and utilization of DRL-funded technologies/activities?

8. Based on your observed experience, do you believe that a disruption to the work of civil society can have a negative impact on the expansion of democratic values and the protection of human rights? Please explain.

9. Based on your observed experience, is emergency support effective for reducing the impacts of digital attacks? What else is important to reduce the impacts of digital attacks?

Looking Ahead

10. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

11. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IMPLEMENTING PARTNER, LOE NO. 8, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your program?

   - Did you develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?

   - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

   - Were there any results or outcomes that surprised you, either positively or negatively?
   -

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #8, Public Awareness Raising and Education

5. Based on your observed experience, to what extent has your organization's program contributed to a better understanding of digital security risks among civil society and the public at large? Please explain.

6. Based on your observed experience, to what extent has your organization's program contributed to improving and scaling educational support services to increase awareness of the potential digital security risks facing civil society and the public at large?

7. Based on your observed experience, which of the following methods of public awareness raising and education are available to civil society and the public at large and effective for improving their understanding of the existing and emerging digital security risks they may encounter ?

   - Individual resources?
   - Localized educational resources?
   - Adult education methodologies promoting digital literacy?
   - Global online training platforms?
   - Curriculum design and standard setting?

- Campaigns?

8. Based on your observed experience, what are the socio-economic and technical barriers to the adoption of better digital security by organizations and the public at large?

9. Based on your observed experience, is digital literacy essential for digital security education? What else is important in order to develop digital security education?

10. Based on your observed experience, why are tailored resources important to civil society and marginalized populations? What else is important to support these groups specifically?

Looking Ahead

11. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

12. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IMPLEMENTING PARTNER, LOE NO. 9, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your program?

   - Did you develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?

   - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

   - Were there any results or outcomes that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #9, Human Rights in Internet Policy

5. Based on your observed experience, to what extent has your organization's program provided human rights defenders access to advocate for human rights in multi-stakeholder technology policy and standards fora? Please explain.

6. Based on your observed experience, to what extent has your organization's program strengthened the capacity of human rights defenders to advocate for human rights in multi-stakeholder technology policy and standards fora? Please explain.

7. Based on your observed experience, to what extent have DRL-assisted civil society organizations successfully advocated for the protection of human rights online?

   - In what type of fora (local, national, regional, global) have DRL-assisted civil society been more effective in advocating for the protection of human rights online?

8. Based on your observed experience, what types of engagements with other stakeholders help or hurt civil society advocacy for human rights online?

9. Based on your observed experience, what types of human rights issues are best advocated by civil society?

10. Based on your observed experience, do your program's-assisted civil society organizations usually lack knowledge, access, or capacity to engage in standards-setting? In what circumstances? What areas of assistance do your program's assisted civil society organizations generally need support in?

11. Based on your observed experience, do your program's assisted civil society organizations usually lack knowledge, access, or capacity to engage in policymaking processes concerning Internet governance? In what circumstances? What areas of assistance do your program's assisted civil society organizations generally need support in?

12. Based on your observed experience, in the context of Internet policy development, is a multi-stakeholder approach important to ensure the Internet is rights-respecting? Why? What else is important?

Looking Ahead

13. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

14. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IMPLEMENTING PARTNER, LOE NO. 12, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your program?

    - Did you develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?

    - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

    - Were there any results or outcomes that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #12, Legal Advocacy

5. Based on your observed experience, to what extent has your organization's program contributed to a greater respect for rule of law that ensures protections of human rights online? Please explain.

6. Based on your observed experience, have you found that the role of strategic litigation can help the exercise of human rights on the Internet?

7. Based on your observed experience, have you found that training law practitioners and judges can help the exercise of human rights on the Internet?

8. Based on your observed experience, are legal challenges effective to address repressive application of the judiciary and law enforcement to restrict human rights online in countries with rule of law?

9. Based on your observed experience, what is the effectiveness of organizations lobbying in congresses for changes and/or improvements within the legal and regulatory environment?

Looking Ahead

10. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

11. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

IMPLEMENTING PARTNER, LOE NO. 13, FGD GUIDE

General Questions

1. Please tell me a bit about your organization's program under the IF Portfolio and its goals towards advancing human rights, specifically freedom of expression and assembly and online privacy.

2. Based on your observed experience, what is the relationship between an open Internet and human rights? Is freedom on the Internet essential for the exercise of human rights?

3. How would or did you define the success of your program?

   - Did you develop a monitoring system or establish indicators to track progress towards these goals? If yes, how did the established system and indicators contribute to understanding the program's success?

   - Is there an example or success story of where progress has been made that you would like to share with the evaluation team?

   - Were there any results or outcomes that surprised you, either positively or negatively?

4. Can you describe your level of engagement, if any, with the IF Portfolio team?

Line of Effort #13, Global Rankings

5. Based on your observed experience, what legal and policy analyses and/or relevant metrics exist to support civil society and human rights defenders in effectively comparing laws, policies, and procedures that respect human rights online across countries and regions?

6. Based on your observed experience, what approaches do civil society and human right defenders use to measure how laws, policies, and procedures respect human rights online? Are these approaches effective? Why or why not?

7. Based on your observed experience, to what extent has your organization's program contributed to creating an objective and comparable metric for laws, policies, and procedures that respect human rights online? Please explain.

8. Based on your observed experience, have the following actions contributed to creating an objective and comparable metrics? What other methods are possible?
   - Evaluation of new threats to Internet freedom?
   - Longitudinal assessments?
   - Country and regional legal/policy analysis?

9. Based on your observed experience, are the legal and policy analyses being conducted actually yielding accurate and applicable research to ensure the respect and protection of human rights online? What is out there to support research development?

10. Based on your observed experience, what are the biggest challenges and barriers to ensuring civil society and human right defenders can measure laws, policies, and procedures and the extent to which they respect and protect human rights online?

11. Based on your observed experience, what are the known or emerging issues that should be considered when designing metrics and measuring these laws, policies, and procedures for civil society and human rights defenders?

Looking Ahead

12. Based on your observed experience, are there any key lessons learned or major takeaways from your work with the IF portfolio that you would like to share?

13. Looking ahead, are there other points of feedback you would like to share that could further improve or strengthen Internet Freedom programming? Are there additional areas of focus that should be addressed or prioritized moving forward?

ANNEX 4. LITERATURE REVIEW

INTRODUCTION

Background and Understanding

The U.S. State Department is in charge of the country's diplomatic and national security interests, preserved through alliances with foreign countries and the propagation of American democratic values. In 2006 the State Department included Internet Freedom in its policy agenda after the Country Reports on Human Rights Practices highlighted a new concern on "the extent to which internet access is available to and used by citizens in each country and (...) whether governments inappropriately limit or block access to the internet or censor websites."[5] In that same year, Secretary of State Condoleezza Rice created the Global Internet Freedom Task Force[6] aiming to "maximize freedom of expression and the free flow of information and ideas", "minimize the success of repressive regimes in censoring and silencing legitimate debate", and "promote access to information and ideas over the internet."[7]

Shortly after, in 2009, the Global Online Freedom Act, established as part of U.S. policy, was enacted to ensure (i) the promotion of freedom to seek, receive, and impart information and ideas through any media; (ii) the use of appropriate instruments of U.S. influence to support the free flow of information without interference or discrimination; and (iii) the detainment of U.S. businesses from cooperating with internet-restricting countries in effecting online censorship. The Foreign Assistance Act of 1961 was also amended to require assessments of electronic information freedom in each foreign country.[8]

However, it was not until 2010 that these ideas and objectives were named *Internet Freedom*. This concept – as adopted by the U.S. foreign policy community – was first presented in Secretary of State Hillary Clinton's 2010 historic remarks through the lens of Roosevelt's Four Freedoms Speech.[9] In a speech delivered the following year, Secretary Clinton admitted that the goal of achieving Internet Freedom was one that the United States Government could not meet on its own: "To maintain an internet that delivers the greatest possible benefits to the world, we need to have a serious conversation about the principles that will guide us, what rules exist and should not exist and why, what behaviors should be encouraged or discouraged and how."[10]

To pursue the ideal of an open internet, U.S. foreign policy needed to work via multilateral and multistakeholder cooperation and engagement. By identifying and empowering allies - even within non-ally

[5] Under Secretary of State for Democracy and Global Affairs Paula Dobriansky, A On-The-Record Briefing on the State Department = S. 2006 Country Reports on Human Rights Practices, Washington, March 6, 2007

[6] U.S. Mission to the United Nations in Geneva. (2006). "Secretary of State Establishes New Global Internet Freedom Task Force," press release. http://geneva.usmission.gov/Press2006/02141InternetTaskForce.html

[7] U.S. Department of State. (2009). Global Internet Freedom Task Force. https://2001-2009.state.gov/g/drl/lbr/c26696.htm

[8] Henry, Ryan, Stacie L. Pettyjohn, and Erin York. "Portfolio Assessment of the Department of State Internet Freedom Program." RAND Corporation, September 4, 2014. https://www.rand.org/pubs/research_reports/RR794.html.

[9] Clinton, Hillary Rodham. (2010). Remarks on Internet Freedom. US Department of State. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

[10] Clinton, Hillary. (2011). Internet Rights & Wrongs: Choices and Challenges in a Networked World. American Rhetoric Online. https://www.americanrhetoric.com/speeches/hillaryclintoninternetpolicyspeechgw.htm

states - the open internet agenda was not only intended to foster American values of freedom, but also to mitigate the increasing cyber risks non-allied countries started to pose against the objectives of the U.S. Clinton's State Department's NetFreedom Task Force, which then directed "U.S. efforts in more than 40 countries to help individuals circumvent politically motivated censorship by developing new tools and providing the training needed to safely access the internet."[11]

More recently, under Pillar IV of the 2018 U.S. National Cyber Strategy—Advance American Influence, which sets as its core objective to "preserve the long-term openness, interoperability, security, and reliability of the internet, which supports and is reinforced by United States interests," Internet Freedom is defined as "the online exercise of human rights and fundamental freedoms — such as the freedoms of expression, association, peaceful assembly, religion or belief, and privacy rights online — regardless of frontiers or medium[12]." By preserving a global open internet, the U.S. strives not only to foster its own values, but also to protect its commercial interests around the world.[13]

In 2020, through the Appropriations Act, 2020, $23,775,000 was directed to programs under this scope. According to the Consolidated Appropriations Act, funding for Internet Freedom programs were to be made available for programs that:

1) focused on countries whose governments restrict freedom of expression on the internet and that are important to the national interest of the U.S.;[14]
2) support the efforts of civil society to:[15]
    - counter development of repressive internet-related regulations, including those originated at international organizations;
    - to combat violence against bloggers and other users;
    - to enhance digital security training and capacity building for democracy activists.
3) have made available research on the topic of Internet Freedom;[16]
4) develop technologies that provide or enhance access to the internet, including circumvention tools.[17]

These targets still resonate with the U.S. Internet Freedom objectives of empowering citizens, providing capacity building, and focusing on developing circumvention technologies established in 2010.

The Internet Freedom Portfolio

As part of these efforts, the United States Department of State (DOS), Bureau of Democracy, Human Rights, and Labor, Office of Global Programming (DRL/GP) launched the Internet Freedom Portfolio. The Internet Freedom Portfolio was designed to advance human rights, including internet freedoms, in accordance with the mandates of the Consolidated Appropriations Act and US National Cyber Strategy, notably in countries where severe or emerging restrictions threaten citizens' abilities to exercise their rights to access the global internet and communicate their thoughts, ideas, and opinions freely. To date, the Internet

[11] Congressional Research Service. (2016). Promoting Global Internet Freedom: Government and Industry Initiatives. CRS Report R41837.

[12] The White House. (2018). "National Cyber Strategy of the United States of America". United States Government, Trump White House Archives.

[13] While these efforts have not been without critics, most democratic countries do welcome the US foreign policy in space.

[14] United States Congress. (2020). Consolidated Appropriations Act, Section 7051(a). United States Government

[15] Ibid.

[16] Ibid.

[17] Ibid.

Freedom Portfolio has implemented nearly 100 programs, of which over 50 remain active, in every region of the world.

DRL/GP commissioned DevTech Systems, Inc. (DevTech) to conduct an evaluation of the Internet Freedom Portfolio to (1) examine the effectiveness of the Internet Freedom Portfolio's overarching strategy and current programming in meeting its established objectives and goals; (2) garner important implementation lessons learned that can be applied to future programming; (3) assess progress at the output and outcome levels; and (4) ascertain any unintended outcomes, whether positive or negative, resulting from programming. As an initial data collection effort, DevTech conducted a Desk and Literature Review to lay the foundation for the evaluation. As part of this effort, the evaluation team:

- Reviewed the Internet Freedom Portfolio's Strategic Framework and its corresponding objectives, values, and goals including those of each individual pillar and line of effort. Please refer to Figure 2 for a detailed overview of the Internet Freedom Portfolio Strategic Framework and Annex 5 for a summary of the Internet Freedom Portfolio lines of effort, theories of change and underlying assumptions. At the program level, the evaluation team reviewed documentation pertinent to the 16 programs selected by DRL/GP to be targeted by the evaluation.

- Reviewed and analyzed other reports produced by Internet Freedom Portfolio's programs and provided to the evaluation team.

- Analyzed products (reports and analyses) of other organizations and development partners in the area of internet freedom, human rights, and the flow and accessibility of online information, and identified possible best practices or lessons learned that could apply to future Internet Freedom programming or strategy design.

- Analyzed international practices and data from international indices relevant to the field of Internet Freedom, human rights, and online information, where appropriate, collected and calculated by well-known, credible international think tanks and agencies.

Please refer to References for a detailed list of the sources reviewed to date.

This following presents the team's preliminary findings gathered through this research effort. The evaluation team will continue to build on these findings throughout the evaluation, organizing information and evidence by evaluation questions to allow for structure data processing and analysis to inform the final evaluation report.

THE PILLARS OF INTERNET FREEDOM

The following section is designed to provide a solid understanding of the existing technical evidence base for which the Internet Freedom Portfolio built the Strategic Framework and the corresponding assumptions that underly each of the four levels of effort and their corresponding theories of change. This information will contribute to answering Evaluation Questions (EQs) one and two.

1) How effective are Internet Freedom Programs completed within the last five years, as assessed against the internet freedom Strategic Framework indicators, values, and goals?

2) How accurate are the assumptions that form the basis of the Internet Freedom Strategic Framework Lines of Effort?

Technology

In recent years, advances in internet and information communication technology have transformed the ways in which individuals' "seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print"[18]. Technology, itself has opened the door to share and obtain information in unprecedented levels – in real time from anywhere in the world – changing the way in which people, communities, and institutions interact.

In 2021, according to the annual Freedom on the Net study led by Freedom House, the world saw, for the 11th consecutive year, a decline in Internet Freedom – signaling the continued deterioration of human rights online and the deepening of digital repression.

According to the World Bank, in 2020 over 60 percent of the world's population had access to and used the internet. [19] This number has only increased over the past two years – in part due to the onset of the COVID-19 pandemic. While these advances in technology have expanded the ways in which individuals are able to exercise their human rights – such as freedom of expression, freedom of assembly, and right to privacy online – technology has also introduced new risks limiting and, in some cases, prohibiting one's ability to enjoy these very same fundamental rights.

Unfortunately, as the world has experienced the expansion of technology, it has also seen the rise of digital authoritarianism and subsequently, censorship (e.g., increasing efforts to take down content and even whole websites)[20], surveillance, and various cyberattacks (e.g., distributed denial of services (DDoS)). Around the

[18] United Nations General Assembly. (1966). International Covenant on Civil and Political Rights, Art. 19. United Nations General Assembly Resolution 2200A. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[19] World Bank. (n.d.). Individuals Using the Internet (% of population). https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2020&start=2020&view=bar

[20] "Data from the past few years show that incidences of global shutdowns have remained steadily high: 196 documented incidents in 2018, 213 incidents in 2019, and 155 in 2020. The first five months of 2021 recorded fifty shutdown incidents." In Feldstein, Steve. (2022). Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond? Carnegie Endowment for

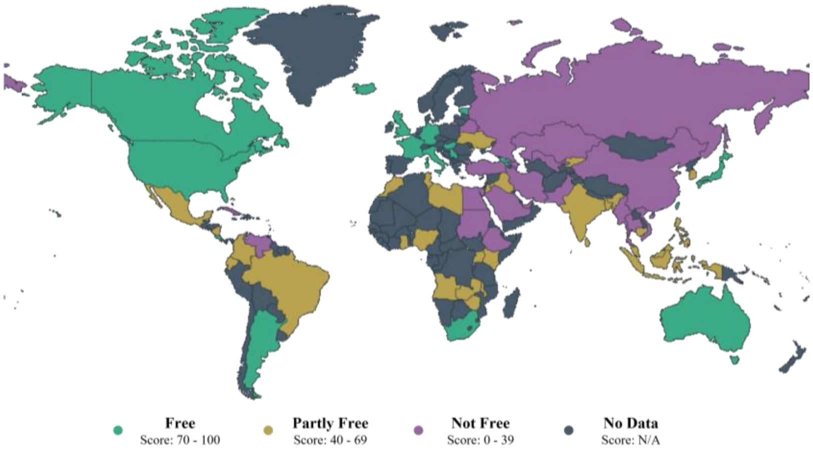
world, millions of people are experiencing the repression of internet freedoms, or the denial of access altogether, as governments restrict their ability to share and access information, filter and/or block content, censor independent media outlets, and promote politically charged disinformation. Increasingly, in times of crises, governments of both authoritarian and democratically-elected regimes are resorting to internet blackouts or shutdowns, declaring these as necessary to ensure public safety and deter the spread of disinformation.[21]

Anti-Censorship Technology

Broadly speaking, internet censorship can be categorized into two major categories (1) the control or suppression of one's ability to publish, post, or share information online and (2) the control or suppression of one's ability to access information online.

Today, internet users, including journalists, human rights activists, and social media account holders, among others, are empowered to publish or share information in a variety of new ways, from posting pictures and videos via social media platforms, to starting a blog, or launching a crowd-funding campaign, without any bias on content or geographic location. At the same time, however, a "growing number of governments are asserting their authority… often forcing [the private sector] to comply with online censorship and surveillance" laws and regulations.[22] For some, this has resulted in imprisonment, physical assault, and/or technical attacks for the non-violent content they post. In 2021, "more governments have arrested [internet] users for publishing nonviolent political, religious, or social speech than ever before. [Internet access has been shut down or suspended in] at least 20 countries and 21 states blocked access to social media platforms."[23] Furthermore, in some countries, users are in danger when they access or even attempt to access certain websites or online services due to government censors and surveillance.

Figure 1. Internet Freedom Status



Source: Freedom House, 2021 Internet Freedom Status

International Peace. https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687#:~:text=Data%20from%20the%20past%20few,2021%20recorded%20fifty%20shutdown%20incidents

[21] Human Rights Watch. "Shutting Down the Internet to Shut Up Critics." In English, 2020. https://www.hrw.org/world-report/2020/country-chapters/global-5

[22] Shabaz, Adrian and Funk, Allie. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

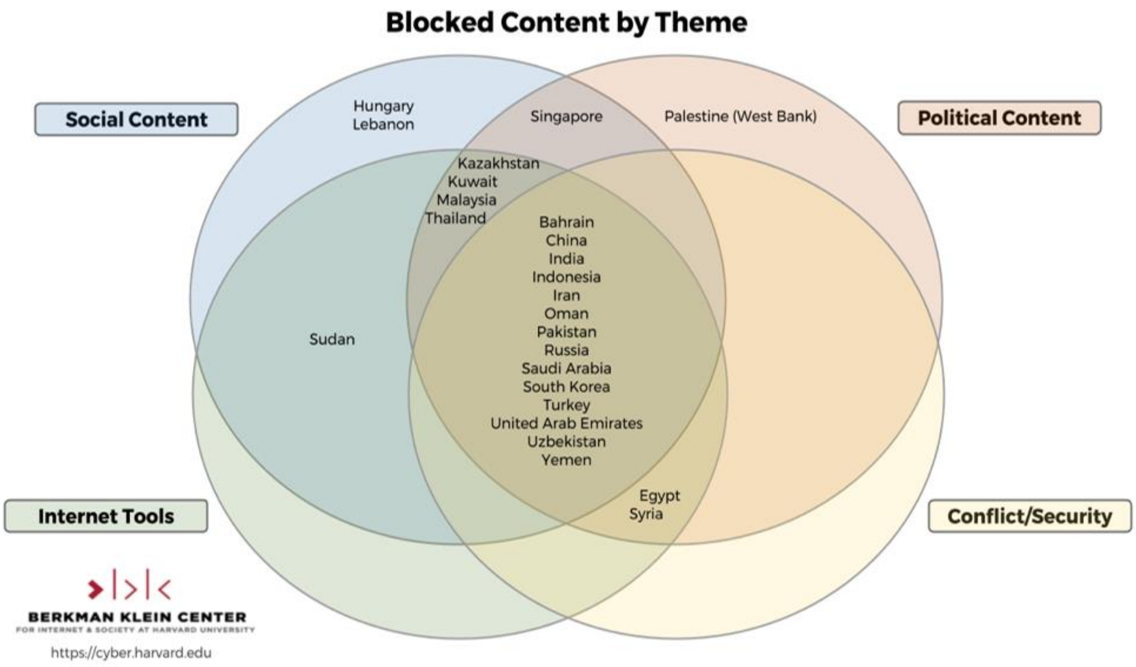
[23] Ibid.

While many states assert that some level of censorship is necessary to mitigate "online harms, rein in misuse of data, or end manipulative market practices," the majority of censorship laws in place "impose excessively broad censorship and data-collection requirements… [where] users' online activities are now more pervasively moderated and monitored by companies through processes that lack the safeguards featured in democratic governance, such as transparency, judicial oversight, and public accountability."[24] In response to these barriers, public and private organizations have and continue to develop anti-censorship and circumvention technology to protect and empower individual citizens, activists, and independent media outlets around the world to use the internet as a platform to voice their ideas, opinions, and concerns and to shed light on the issues surrounding online censorship.

Common Types of Censorship Technology

- Distribution Network
- Tampering
- IP Blocking
- Keyword Filtering
- Packet Filtering
- Performance Degradation
- DDoS

Figure 2. Blocked Content by Theme



Source: https://today.law.harvard.edu/new-berkman-klein-center-study-examines-global-internet-censorship/

Anti-censorship and circumvention technology is designed to bypass the filtering schemes and blocks often put in place by governments and thus allow users to access information and share content more freely. This

[24] Shabaz, Adrian and Funk, Allie. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

technology comes in a variety of forms such as virtual private networks, traffic obfuscation technologies, mesh networks, IP tunneling, re-routing, domain fronting, and browser-based proxies, among others.[25, 26] According to existing research and best practices, the success of anti-censorship and circumvention technology relies heavily on its ability to ensure privacy or anonymity, to protect the provided content, and to sufficiently distribute the filtering of content. The success of these tools can also be attributed to their user-centered design that ensures that the intended users can readily access these technologies at little to no cost. In addition, according to the Consolidated Appropriations Act, many of these tools are verified against industry standards through a security audit conducted by an independent third-party.

In recognition of these challenges, under its Technology pillar, the Internet Freedom Portfolio strives to support the development and accessibility of open source, interoperable, and transparent technologies to promote anti-censorship and the exercise of human rights as well as the flourishing of democratic principles. The evaluation sample contains two Internet Freedom Portfolio programs designed to address censorship and promote freedom of expression: (1) Technology Project B and (2) Technology Project A. The Technology Project Bbuilt a decentralized content distribution network that allows web-based and mobile applications to get content through secure peer-to-peer distribution. Technology Project A on the other hand, advanced anti-censorship by bringing a well know and highly evaluated circumvention tool to more users at lower cost.

Secure Communications

Technology has provided opportunities to communicate and share ideas on a global scale. For over a decade, many countries, including the U.S., have promoted internet freedom in effort to achieve, as Secretary Clinton stated, "one internet, one global community, and a common body of knowledge that benefits and unites us all."[27] However, human rights laws and technology regulations have struggled to maintain pace with the rapidly evolving online ecosystem, particularly with respect to the expansion and use of technology for surveillance and the protection of one's privacy through secure communications.

According to the Universal Declaration of Human Rights Article 12, privacy is among the fundamental human rights recognized by international law. In addition, one's individual privacy is "central to the maintenance of democratic societies" and the assurance of human dignity.[28] Yet, as the internet has forever changed the way in which the world shares and receives information, governments and internet users alike have struggled to put clear boundaries on what information should be protected. According to the U.S. Government, personal identifiable information "refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[29] With regard to internet use, protected information is "all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public…"[30] This includes

[25] Human Rights Watch. "Shutting Down the Internet to Shut Up Critics." In English, 2020. https://www.hrw.org/world-report/2020/country-chapters/global-5

[26] Cui, Jingbo. (2021). Network Censorship. McKelvey School of Engineering, Computer Science & Engineering. https://www.cse.wustl.edu/~jain/cse570-21/ftp/pearg.pdf

[27] Clinton, Hillary Rodham. (2010). Remarks on Internet Freedom. US Department of State. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

[28] Necessary & Proportionate. (2014). International Principles on the Application of Human Rights to Communications Surveillance. https://www.eff.org/files/necessaryandproportionatefinal.pdf

[29] USAID. Privacy Basics. (2014). United States Government. https://www.usaid.gov/sites/default/files/documents/1868/508saa.pdf

[30] Necessary & Proportionate. (2014). International Principles on the Application of Human Rights to Communications Surveillance. https://www.eff.org/files/necessaryandproportionatefinal.pdf

information that can individually or collectively be used to "reveal a person's identity, behavior, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event."[31]

Today more than ever, internet surveillance is being used to collect user data and track user behavior, including protected information. The surveillance market, and the growing incentives for obtaining user information, is giving more leeway to governments "than ever before to flout the rule of law, monitor private communications at their own discretion…"[32] The *Freedom of the Net* 2021 report found that nearly 65 percent of the 70 countries surveyed "… are suspected of having access to sophisticated spyware or data-extraction technology supplied by secretive companies…"[33] Social media platforms and other communication networks once considered to be champions in promoting human rights through freedom of expression are now seen as key contributors to an increasingly unsafe and insecure online environment. In recent years, these platforms and networks have experienced a rise in "data leaks, ransomware attacks, a wave of misinformation and disinformation, and various cybersecurity incidents that have made us all feel less safe and, often, less free."[34] While accessibility and freedom of expression through free internet or the use of anti-censorship technology are important priorities for many internet users, government and state actors are increasingly using the need to protect the safety of the public online as a rationale for identifying and monitoring illegal and potentially harmful content. For example, the United Kingdom's Online Safety Bill recently presented to Parliament for approval promises to create an online environment that is "safer for users and holds tech giants to account."[35] While this initiative, among others, is thought by many to be a monumental step forward in addressing public threats and the security of the internet, some argue that prioritizing internet safety is "inward-looking, fragmented – and often dangerously misguided" and is often motivated by a desire to control global communication.[36] This calls into question whether efforts to promote internet security and safety are in support of or in opposition to one another – and which of the two, if either, ensure one's human rights. As governments seek to prioritize safety by establishing new laws and conditions, it is becoming increasingly difficult for tech developers to prioritize security for internet users. Research suggests that in addition to monitoring users' behaviors, user privacy has historically been compromised as significant amounts of identifiable information, including IP address information, are revealed.[37]

In efforts to ensure secure communications and to promote human rights and democratic change, the Internet Freedom Portfolio seeks to develop and support technologies that promote surveillance-free communications, particularly for human rights defenders and the media. One such example is Technology Project C. By working directly with tool developers, Technology Project C sought to pioneer the way in which open-source privacy and security tool developers, digital security trainers, and at-risk users think about usability, accessibility, and feedback by integrating marginalized and vulnerable communities including journalists, human rights defenders; lesbian, gay, bisexual, transgender, and intersex (LGBTI) individuals; women; and, other minorities into the development process.

[31] Ibid.

[32] Repucci, Sarah and Slipowitz, Amy. (2022). The Global Expansion of Authoritarian Rule. Freedom House. https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

[33] Shabaz, Adrian and Funk, Allie. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

[34] Komaitis, Konstantinos. (2021). Internet Safety Is the New Internet Freedom. Slate. https://slate.com/technology/2021/11/internet-safety-vs-internet-freedom.html

[35] Government of the United Kingdom. (2022). Press Release: World-first online safety laws introduced in Parliament. https://www.gov.uk/government/news/world-first-online-safety-laws-introduced-in-parliament

[36] Komaitis, Konstantinos. (2021). Internet Safety Is the New Internet Freedom. Slate. https://slate.com/technology/2021/11/internet-safety-vs-internet-freedom.html

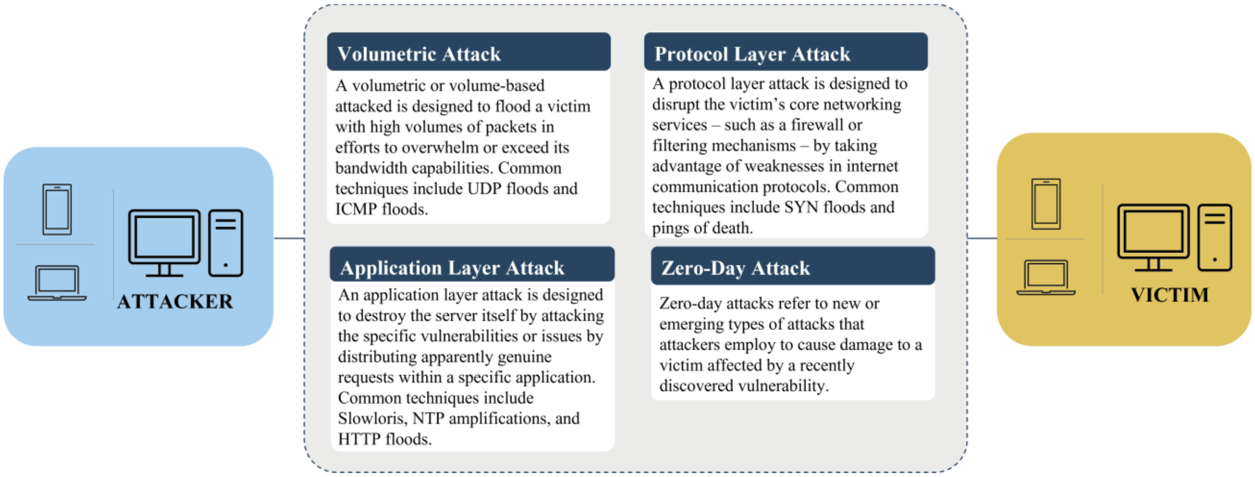
[37] Leberknight, Christopher, et al. (2010). A Taxonomy of Internet Censorship (Draft Version). http://www.princeton.edu/~chiangm/anticensorship.pdf

Distributed Denial of Service (DDoS) Mitigation

Among the many types of cyberattacks, DDoS attacks are the most common and disruptive. A DDoS attack is a "malevolent attempt to make an online service unavailable to genuine customers by simply stopping or delaying the host server's service." [38] Over the past few years, these types of cyberattacks have only "grown in both number and sophistication with the rise of advanced wireless technology and modern computing paradigms."[39]

In simple terms, a DDoS attack is initiated when an attacker sends a malicious packet to a specific or targeted server, known as the victim. These packets flood victim's workstations with requests to disrupt their system and deplete their resources to the point where the server begins to slow down and, in many cases, crashes or "shuts down altogether, preventing normal use and system access."[40] The following figure highlights some of the most common strategies and types of digital attacks, including DDoS attacks, used today.

Figure 3. Common Strategies and Types of Digital Attacks



Volumetric Attack

A volumetric or volume-based attacked is designed to flood a victim with high volumes of packets in efforts to overwhelm or exceed its bandwidth capabilities. Common techniques include UDP floods and ICMP floods.

Protocol Layer Attack

A protocol layer attack is designed to disrupt the victim's core networking services – such as a firewall or filtering mechanisms – by taking advantage of weaknesses in internet communication protocols. Common techniques include SYN floods and pings of death.

Application Layer Attack

An application layer attack is designed to destroy the server itself by attacking the specific vulnerabilities or issues by distributing apparently genuine requests within a specific application. Common techniques include Slowloris, NTP amplifications, and HTTP floods.

Zero-Day Attack

Zero-day attacks refer to new or emerging types of attacks that attackers employ to cause damage to a victim affected by a recently discovered vulnerability.

Recent literature suggests that the internet can be used be used as either a "liberation technology" empowering citizens and marginalized groups from authoritarian and repressive regimes or as a tool of digital repression, enhancing the abilities of governments to censor information and surveil online users. Similarly, DDoS attacks can reflect dual characteristics such that "governments or state-near groups can use them to censor and temporarily disable unwanted outlets, while activists can use DDoS attacks as a new tool to attack state servers."[41] This is especially apparent around political events or focal points – such as elections and the release of new legal and regulatory reforms.

[38] Ammarah Cheema, Moeenuddin Tariq, Adnan Hafiz, Muhammad Murad Khan, Fahad Ahmad, Muhammad Anwar, "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review", Security and Communication Networks, vol. 2022, Article ID 8379532, 15 pages, 2022. https://doi.org/10.1155/2022/8379532

[39] Jassem, Manal Dawood, Amer Abdulmajeed Abdulrahman. (2022). Survey on Distributed Denial of Service Attack Detection Using Deep Learning: A Review. Int. J. Nonlinear Anal. Appl. In Press, 1 – 10. ISSN: 2008-6822. https://ijnaa.semnan.ac.ir/article_6458_8d4fe99cb1b53f375c13856578dbacf9.pdf

[40] Ammarah Cheema, Moeenuddin Tariq, Adnan Hafiz, Muhammad Murad Khan, Fahad Ahmad, Muhammad Anwar, "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review", Security and Communication Networks, vol. 2022, Article ID 8379532, 15 pages, 2022. https://doi.org/10.1155/2022/8379532

[41] Lutschuer, Philipp M., Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti. (2020). At Home and Abroad: The Use of Denial-of-service Attacks during Elections in Nondemocractic Regimes. Journal of Conflict Resolution 2020, Vol.64(2-3) 373-401. https://journals.sagepub.com/doi/pdf/10.1177/0022002719861676

While it is impossible to prevent an attacker from launching a DDoS attack on a victim, research shows that there are several key steps one can take to reduce the risk and potential effects of an attack.[42,43] These include:

1) Conduct a **DDoS Risk Assessment** to understand one's existing vulnerabilities and develop a **DDoS Response Plan** or incident response plan that provides clear step by step instructions on what to do when encountering a DDoS attack. For organizations, this should include, at a minimum, team member roles and responsibilities, escalation protocols, and a list of mission-critical systems. The plan must be reviewed regularly and updated, as needed. In addition, it should be accessible to staff and may include security awareness trainings.

2) Establish tactics to ensure **high levels of network security** including but not limited to, firewalls and intrusion detection systems, anti-virus and anti-malware software, web and endpoint security tools, network segmentation, and reverse proxies such as content delivery networks, autonomous system numbers, and web application firewalls, as well as network infrastructure to prepare for traffic spikes.
3) **Continually monitor** traffic to detect an attempt before an attack, identify normal trends in user activity and traffic to recognize malicious patterns or warning signs more easily, and "develop the intelligent, adaptive defenses you need to fend off future attacks."[44]

In response the escalation of DDoS attacks, the Internet Freedom Portfolio seeks to develop and promote technologies that equip human rights defenders, civil society groups, and independent media outlets with the tools to ensure the delivery of critical content via resilience websites. Notably, as part of this evaluation, Technology Project D, sought to enhance machine learning toolkits and time-series anomaly prediction systems – in collaboration with strengthening civil society's capacity – to detect emerging threats online more readily and ultimately, to prevent and mitigate DDoS attacks more effectively. In addition, Technology Project D worked to expand and strengthen the attack mitigation infrastructure in effort to make DDoS attacks "more expensive, less effective, and to peel away at attackers' impunity by enabling attribution."[45]

Digital Safety

Despite an increase in the availability of technology and resources designed to help individuals protect their personal information online and respond to imminent threats, there is a growing understanding that technology alone cannot protect people's digital security. Ultimately, as online users are the ones who choose to and need to know how to adhere to security procedures, if users themselves do not properly deploy and utilize the available technologies, their digital safety is at risk. This is particularly the case for human rights defenders worldwide, especially for those in countries with extreme levels of surveillance and for those who have limited resources. As the race between technology that protects and technology that harms is constantly evolving, it is essential that users understand the advantages, disadvantages, and limitations of these technologies, such as Signal or Tor, and their intended use as well as the recommendations and guidelines on how to protect one's digital privacy and identify, which are often "hard to understand or act on."[46] Such

[42] Five Best Practices for Mitigating DDoS Attacks: How to defend against rapidly evolving Distributed Denial-of-Service threats and address vulnerabilities at every layer. (2020.) Cloudflare. https://www.cloudflare.com/resources/assets/slt3lc6tev37/bNnFz1PMZtHvYsCWrl3n1/fe46ed61db9ee7d9e4466484d6612de7/Five-Best-Practices-for-Mitigating-DDoS-Attacks-WP.pdf

[43] Velimirovic, Andreja. (2021). How to Prevent DDoS Attacks: 7 Tried-and-Tested Methods. PhoenixNAP. https://phoenixnap.com/blog/prevent-ddos-attacks

[44] Ibid.

[45] DRL Scope of Work – Cost Extensions. DOC001099775_12.1_Updated_Scope_of_Work

[46] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23

information is widely available across the internet, in “formats ranging from mobile apps, video, and animation through to plain text.”[47] However, while readily available, information can easily misguide users due to contradictory recommendations among sources. In addition, resources are often available in a limited number of languages reducing the accessibility of information.[48] Even when an individual does grasp how to protect themselves online, new threats and online risks are always emerging, requiring the user to constantly review and refresh their understanding of security procedures and their options for technology that supports their digital safety.

Beyond individual online users, the need for digital safety also extends to and intensifies at the organization level. For organizations, including philanthropic, civil society, and human rights organizations, digital security is of upmost importance as they are often the target of digital attacks. Thus, these organizations have different needs considering they have higher security risks and face different “threat models” than individuals due to their specific systems used to “store, share, and process user data, as well as the communication platforms, networks, and devices staff and constituents use” to share information.[49] At the same time, implementing digital safety measures into an organization involves “changing habits, retrofitting old systems and policies,”[50] changing behaviors that can put people and data at risk[51] and most of all, requires changing “traditional ways of thinking”[52] from both funders and donors of these organizations. Such efforts represent large transactional costs, and require large financial resources and profound cultural change and time – all potential obstacles to digital safety implementation within the context of fast paced technology development.

Digital Security Capacity Building

In efforts to address these challenges and ensure the digital security and resilience of both individuals and organizations, specifically those engaged in philanthropic, civil society, and human rights organizations, targeted and holistic capacity building programs and activities are considered to be critical elements to developing a culture or ecosystem that upholds internet freedom. Capacity building efforts often present themselves in a diverse set of techniques and approaches, yet research suggests that to ensure safe operations online, the following four characteristics are critical to success:[53]

1) **Commit to digital security as essential to all work.** According to a McKinsey Cybersecurity report from 2019, business leaders already consider cyber risk “as important a priority for the leaders of public and private institutions as financial and legal risks.”[54]

2) **Take big responsibility for big data.** Since philanthropic, civil society and human rights organizations are common targets for digital attacks as they often maintain large datasets with personally identifiable information from third parties – from donors to the beneficiaries of their program, in addition to advocacy coalitions – these organizations require proper security and management lest the organization and their community become at risk.

[47] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). “Building Digital Safety for Journalism: A Survey of Selected Issues.” UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi
[48] Ibid.
[49] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23
[50] Ibid.
[51] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). “Building Digital Safety for Journalism: A Survey of Selected Issues.” UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi
[52] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23
[53] Ibid.
[54] Boehm, Jim, Peter Merrath, Thomas Poppensieker, Rolf Riemenschnitter, and Tobias Stahle. (2018). Cyber Risk Measurement and the Holistic Cybersecurity Approach. Mckinsey. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach

3) **Prioritize capacity-building as a systemic approach to an organization's overall security.** Only when digital safety capacity building efforts are integrated into an organization's overarching framework via a systemic approach will organizations be able to effectively address "moving targets like network vulnerabilities, policies governing the sharing of personal data at border-crossing or online surveillance."[55]

4) **See the shared threat as a call for interdependence.** It takes a multistakeholder effort to bring digital security front and center into the work of philanthropic, civil society and human rights organizations. It is a "communal responsibility, rather than an individual responsibility or something that only high-risk groups shoulder."[56] Donors, grantees, nonprofit groups, and activists need to be ready to engage both with their peers as well as with organizations and initiatives that are prepared to offer support, guidance, and collaboration on how one should prioritize digital safety.

Similarly, a more systemic and holistic approach to digital security capacity building is also emphasized by UNESCO's *Building Digital Safety for Journalism* report (2015). The report stresses that ad-hoc training alone is insufficient, and that a holistic approach to digital safety must be comprised of several dimensions, including normative and psychosocial dimensions.[57] Organizations demonstrating higher levels of digital safety most commonly provide capacity building programs that establish and uphold core capacities, including but not limited to[58]:

- Comprehension of international normative standards relevant to freedom of expression and how those are aligned with the work of human rights activists, journalists, and organizations in monitoring, reporting and advocacy activities;
- Understanding of the legal landscape of digital security as well as an understanding of how networks work;
- The ability to assess risk or threats according to vulnerabilities of the organization and the ability to manage them;
- Mitigation strategies;
- An emphasis on developing adaptable skills that can be adjusted to meet specific security situations; and,
- A continuous learning spirit.

Furthermore, organizations can better protect their information and ensure their resilience to imminent threats by becoming a member of a wider cyber capacity building community, allowing them to take part in and contribute to coordination efforts and knowledge-sharing opportunities.[59] This also holds true in the private sector. According to World Economic Forum's *Global Risks Report of 2022*,[60] "cooperation between organizations could unlock best practices that can be replicated across industries and economies" when it comes to digital security. Multistakeholder support is also necessary for sustained learning and the implementation of a security culture as these dialogues are crucial to strengthening links between actors, and

[55] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23

[56] Ibid.

[57] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi

[58] Ibid.

[59] Collett, Robert, Nayia Barmpaliou, Patryk Pawla. (2021). International Cyber Capacity Building: Global Trends and Scenarios. European Commission. https://www.iss.europa.eu/content/international-cyber-capacity-building-global-trends-and-scenarios

[60] World Economic Forum. (2022). The Global Risks Report 2022. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

"at the organizational level, upskilling leaders on cybersecurity issues and elevating emerging cyber risks to board-level conversations will strengthen cyber-resilience."[61]

In addition to an organization's cultural development and capacity to promote digital safety and its ability to effectively reduce the frequency and intensity of digital attacks, coordination – both internally and externally – is of central importance to ensuring that philanthropic, civil society and human rights organizations achieve digital safety. In the absence of coordination, the effectiveness of an organization's digital safety and the safety of the human rights sector cyber security overall, is at risk.[62,63] Thus, a best practice would suggest that when programs and initiatives are designed to offer support, guidance, and collaboration to promote digital security at the individual or organizational levels, these efforts should draw on the donors' collective experiences, approaches, and practices spanning multiple communities, contexts, and countries.[64]

In efforts to improve organizations' digital safety practices and mitigate the impacts of potential attacks, and the impacts to the communities they serve, the Internet Freedom Portfolio provides targeted support to strengthen organizational capacities and skills as well as digital literacy. The Internet Freedom Portfolio evaluation sample includes two programs under the Digital Safety Pillar: (1) Digital Safety Project B and (2) Digital Safety Project A. It is worth stating that both Digital Safety Project B and Digital Safety Project A directly or indirectly rely on core principles and best practices of digital safety: community building and knowledge sharing.

In 2016, the Internet Freedom Portfolio awarded Digital Safety Project B. Among other objectives, Digital Safety Project B supported groups with security frameworks that can be replicated for the community they are part of and the community that supports them. Digital Safety Project B adapted an audit framework that through testing and risk assessment evaluates how digitally safe large organizations are and promotes the necessary training to strengthen their digital safety. The program also assessed public and private donor standards for risk mitigation strategies and provided recommendations and templates to improve risk management in these organizations. By fostering a community of implementers and establishing a fellowship program to integrate the audit framework with existing partner programs and existing organization practices, Digital Safety Project B developed tailored trainings for 10 civil society organizations (CSOs). These programs were designed to strengthen the resilience of these organizations through risk assessments and delivering education services focused on understanding risk.

Complementary to Digital Safety Project B, Digital Safety Project A provided a customized risk mitigation strategy to philanthropic, civil society and human rights organizations by linking them to private cybersecurity firms. This strategy allowed for the possibility of keeping the broader security community that supports organizations informed about emerging threats and attacks and allowed the sharing of solutions. The assumption is that by supporting a strong and coordinated community – as opposed to only fostering the safety abilities of individual organizations – the organizations will be more resilient.

2.2.2. Emergency Support

Human rights activists and free-press journalists disseminate information that is crucial to the propagation of democratic values and the exercise of rights, educating audiences, and promoting transparency. They frequently serve as a powerful and essential voice in communities, acting as "watchdogs, scrutinizing the

[61] World Economic Forum. (2022). The Global Risks Report 2022. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[62] Collett, Robert, Nayia Barmpaliou, Patryk Pawla. (2021). International Cyber Capacity Building: Global Trends and Scenarios. European Commission. https://www.iss.europa.eu/content/international-cyber-capacity-building-global-trends-and-scenarios

[63] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23

[64] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23

formulation of public policy and highlighting blocks to development such as corruption, human rights abuses or inefficient governance."[65] Despite human rights activists' dependence "on the internet and mobile phones to carry out their work," they often have limited access to reliable "resources to protect themselves against spyware deployed by powerful governments."[66] Attacks most commonly suffered by human rights activists and other vulnerable group range from "confiscation or theft of digital resources, online intimidation, disinformation and smear campaigns"[67] to physical and verbal threats to an individual and their families, including death threats, to the loss of one's life.

As important as it is to provide education and invest in a community, as well as investigate and identify who is behind such attacks – to support resilience and long term positive change toward safety – it is as important to offer immediate emergency support – sometimes life-saving support - for those being attacked and threatened.[68] Globally, there is an increasing demand for emergency support services for those under threat of attacks, including support related to physical safety, and/or fast financial, legal and technical support. For the latter, while there are still challenges to approximate journalists and "technologists willing and able to assist them if they experience a digital threat or attack"[69], progress has been made. For instance, the Open Tech Fund provides emergency support services, including organizational security and digital security support, digital attacks response and forensic analysis, web-hosting and connectivity issues response.[70] Amnesty Tech and the Committee to Protect Journalists[71] provide technology services and a mobile verification kit to assess if "one's phone has been targeted."[72] Another key strategy organizations have developed to support others is the development of digital security helplines that connect those "experiencing digital attacks or network with local facilities or actors who may be able to assist."[73] One such example is the Digital Security Helpline offered by Access Now.[74]

Considering that digital safety measures represent a matter of constant vulnerability and struggle for both individuals and organizations – such as human rights activists, among other vulnerable groups and organizations alike – widely available and reliable emergency resources and support services are essential to empower activists to continue their work and to be able to withstand threats and attacks. Two Internet Freedom programs are part of the evaluation sample: including (1) Digital Safety Project C and (2) Digital Safety Project D. Digital Safety Project C strived to improve the accessibility of emergency resources to prevent and mitigate digital attacks. Through emergency support, knowledge, and community building, Digital Safety Project C's programs were designed to promote flexibility, supporting organizations and individuals that face digital threats, which are often fast-changing in nature. Digital Safety Project C's holistic support to individuals or groups under attack or threat thus aimed to create a "resilient networks of support

[65] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi

[66] Lamensch, Marie. (2021). For Rights Defenders, Cyber Is the New Battleground. Centre for International Governance Innovation. https://www.cigionline.org/articles/for-rights-defenders-cyber-is-the-new-battleground/

[67] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi

[68] Weinberg, Friedhelm. (2019). 3 ways activists are being targeted by cyberattacks. World Economic Forum. https://www.weforum.org/agenda/2019/05/3-ways-activists-targeted-online-cybersecurity/

[69] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi.

[70] Open Technology Fund. (n.d.). Rapid Response Fund. https://www.opentech.fund/funds/rapid-response-fund/

[71] Committee to Protect Journalists. (2022). Digital Safety Kit. https://cpj.org/2019/07/digital-safety-kit-journalists/

[72] Lamensch, Marie. (2021). For Rights Defenders, Cyber Is the New Battleground. Centre for International Governance Innovation. https://www.cigionline.org/articles/for-rights-defenders-cyber-is-the-new-battleground/

[73] Lamensch, Marie. (2021). For Rights Defenders, Cyber Is the New Battleground. Centre for International Governance Innovation. https://www.cigionline.org/articles/for-rights-defenders-cyber-is-the-new-battleground/ and Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi.

[74] Access Now. (n.d.). Digital Security Helpline. https://www.accessnow.org/help/

to human rights defenders"[75] Digital Safety Project D, on the other hand, focused on delivering proactive services including performing security audits, forensic analysis of digital attacks and digital mentorship. In addition, the program also provided circumvention services for blocked websites.

2.2.3. Public Awareness Raising and Education

Public awareness and education are also key factors to ensuring a safe and rights-respecting digital ecosystem for all. Increasing awareness and promoting digital literacy helps strengthen the public's understanding of how the actions of governments or third parties and how technology works (or does not work) can affect their digital life and rights – positively or negatively. In some cases, public awareness and education are also crucial to involve citizens in core moments where policy change is needed.

Over the years, citizens around the world have gathered in support of better digital rights, including freedom of expression and of privacy. The Arab Spring in 2011, the 2012 protests against ACTA, and the Net Neutrality fight in the U.S. in 2017, among many others, are key examples of how large campaigns can be used to bring about greater awareness to repressive policies and constraints against one internet freedoms.

Recently, an increasing number of donors and organizations have dedicated resources to raising public awareness and providing education to address the misaligned perception of how individuals' rights are being affected by policies and regulations. When users become more literate on key issues – such as censorship, surveillance, and content manipulation – "they often take actions that enhance internet freedom and protect fellow users."[76] In addition, as recommended by UNESCO in the *Building Digital Safety for Journalism* report (2015), by raising the public's awareness of evolving digital threats, one will organically see an increase in "market demand for digital security tools,"[77] further contributing to strengthening internet freedoms. Likewise, Freedom House's *Freedom on the Net 2021 - The Global Drive to Control Big Tech 2021* report states that "civil society groups should engage in innovative initiatives that inform the public about government censorship and surveillance, as well as investigate and expose disinformation campaigns, including their origins and objectives."[78] It also suggests that governments "should invest in digital literacy training through public education, public service advertising campaigns, and other mechanisms to target individuals from all age groups and socioeconomic backgrounds"[79] as a way to address unequal access to the internet, which increases social inequality, and to foster a more diverse information space.

Furthermore, in alignment with these perspectives, the *Open Internet for Democracy Advocacy Playbook* (2018) suggests potential tactics towards building digital literacy within a community. These include[80]:

- Train school or university teachers;
- Hold meet-ups with target audiences or communities;
- Build online courses or learning platforms;
- Create accessible and inclusive knowledge;

[75] Digital Safety Project C. Project Document on file with evaluation team.

[76] Shabaz, Adrian and Funk, Allie. (2020). Freedom on the Net 2020: The Pandemic's Digital Shadow. Freedom House. https://freedomhouse.org/report/report-sub-page/2020/policy-recommendations-freedom-net-2020#:~:text=Studies%20and%20surveys%20have%20shown,back%20against%20shutdowns%20and%20censorship.

[77] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi.

[78] Shabaz, Adrian and Funk, Allie. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

[79] Ibid.

[80] Open Internet for Democracy. (2021). "Open Internet for Democracy Advocacy Playbook." https://openinternet.global/resources/open-internet-playbook.

- Create methods for continuous engagement;
- Post relevant and engaging content on digital rights for an online community;
- Share training materials and platforms.

In addition to the recommendations and efforts mentioned above, literature also points to two other key factors as crucial to generating the desired impacts of a digitally literate public: community-building and coordination of efforts.[81]

While toolkits, guidelines, web-based and mobile applications, and other technology-based applications are necessary tactics and strategies for raising public awareness and improving digital literacy, they are only effective if utilized. For instance, UNESCO's *Building Digital Safety for Journalism* report (2015) suggests that even those who are already digitally literate still "perceive that the benefits of online social networking outweigh the risks of disclosing personal information."[82] The report suggests that is not unusual to find discrepancies "between users' reported understanding and caution in regard to privacy and [how users are] actually implementing specific steps to maintain privacy."[83] Even though these users are allegedly familiar with privacy tools, their behavior might suggest otherwise. This "lack of usability and [in some cases] accessibility … increases the gap between tech makers and users… [and contributes to greater] misunderstandings of tool functionalities… [often resulting in] a false sense of privacy and security."[84] And since "many of these software development teams are in need of assistance to make tools that are truly usable and accessible in various contexts across diverse communities"[85] venues, such as the Digital Safety Project E conference, Rights Con and the Mozilla Fest, have focused on increasing diversity and inclusion, emphasizing the participation of underrepresented populations and creating opportunities for engagement and learning between technical community and the human rights and digital rights community.

Among the donors contributing to increasing public awareness and education on digital security – notably the promotion of diversity and inclusive approaches, is the DRL/GP Internet Freedom Portfolio, specifically its (1) Digital Safety Project E and (2) Digital Safety Project F. Digital Safety Project E was designed to build a collaborative environment to foster community-building between developers and the users of their tools. By assessing users' needs, developers sought to strengthen the support provided and catalyze usability, decreasing the learning curve and transaction costs related to the mass adoption of digital security tools by the public at large. Similarly, the Digital Safety Project F is an open-source app that seeks to "improve the accessibility, localization and implementation of digital and physical security for human rights defenders" [86] by providing a "user-friendly, easily accessible tool that delivers simple answers on how to operate in any situation." [87]

[81] Collett, Robert, Nayia Barmpaliou, Patryk Pawla. (2021). International Cyber Capacity Building: Global Trends and Scenarios. European Commission. https://www.iss.europa.eu/content/international-cyber-capacity-building-global-trends-and-scenarios

[82] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi.

[83] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi.

[84] Open Technology Fund. (n.d.). Secure Usability and Accessibility Lab. https://www.opentech.fund/labs/sua-lab/

[85] Open Technology Fund. (n.d.). Secure Usability and Accessibility Lab. https://www.opentech.fund/labs/sua-lab/

[86] Digital Safety Project F. Scope of Work.

[87] Digital Safety Project F. Proposal.

Policy Advocacy

Human Rights in Internet policy

Human rights are inherent to all human beings; differences in race, sex, nationality, religion, or any other status or designation do not alter the universal applicability of fundamental human rights.[88] In the context of the internet, emerging policy principles "that describe features of the system which are required to support human rights" are increasingly being developed.[89] The (1) 2016 amendment to Article 19 of the Universal Declaration of Human Rights, (2) the Charter of Human Rights and Principles for the Internet by the Internet Rights & Principles Dynamic Coalition, and (3) the Declaration for the Future of the Internet, an international statement signed by over 60 countries, including the United States, to mention a few, all reflect growing international interest in the connection of human rights and internet policy. They begin to enumerate the principles, practices, and responsibilities of various actors within this policy area.[90] Policy advocacy around issues of human rights in internet policy focuses on identifying and promoting these policy principles with an array of stakeholders to strengthen human rights protections on the internet. Governments remain a principal player in setting policy to enshrine respect for human rights on the internet, but the private sector, civil society, donors, the technical community, and the public at large are further identified as critical actors in policy development and monitoring policy adherence.

Advocating for human rights in internet policy is and will remain critical. Internet freedom has declined for the 11th consecutive year in 2021, as measured by the annual Freedom House study Freedom on the Net.[91] Taking Kyrgyzstan as an illustrative example—and noting this is a country where both sampled programs related to this line of effort are operating—its internet freedom score fell from 65 in 2016 to 53 in 2021 (out of a maximum possible score of 100). The Kyrgyzstani state's involvement in internet policies, development processes, and regulatory bodies is driven by political interests and is largely characterized by a lack of transparency, democratic values, and respect for international human rights norms. These challenges pose obstacles to access, (which scored 13 out of 25 points), and are particularly troubling for user rights, (which scored 17 out of 40 points).[92] Similarly, many governments expand their manipulation of the internet during elections, civil discontent, or unrest. Taking India as an example, these tactics can include outright shutdowns—India led the world in internet shutdowns with 109 in 2020—as well as more subtle actions like "throttling a URL to dramatically slow its function, blocking particular internet addresses, and restricting the use of mobile data."[93] These actions violate democratic values and international human rights norms.

[88] United Nations. (n.d.). Human Rights. https://www.un.org/en/global-issues/human-rights

[89] Internet Rights and Principles Coalition. (2014). The Charter of Human Rights and Principles for the Internet. Internet Governance Forum, United Nations. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf

[90] Internet Rights and Principles Coalition. (2014). The Charter of Human Rights and Principles for the Internet. Internet Governance Forum, United Nations. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf . See also Engler, Alex. (2022). The Declaration for the Future of the Internet is for wavering democracies, not China and Russia. Brookings. https://www.brookings.edu/blog/techtank/2022/05/09/the-declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/ and United Nations General Assembly, Human Rights Council. (2016). Oral Revisions of 30 June. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

[91] Shahbaz, A. & Funk, A. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

[92] Freedom House. (2021). Freedom on the Net 2021: Kyrgyzstan. Freedom House. https://freedomhouse.org/country/kyrgyzstan/freedom-net/2021

[93] Ryan-Mosley, Tate. (2021). Why you should be more concerned about internet shutdowns. MIT Technology Review. https://www.technologyreview.com/2021/09/09/1035237/internet-shutdowns-censorship-exponential-jigsaw-google/?utm_source=pocket_mylist. See also, Human Rights Watch. "Shutting Down the Internet to Shut Up Critics." In English, 2020. https://www.hrw.org/world-report/2020/country-chapters/global-5

In this context, effective internet policy development is understood as a *communal* and multistakeholder[94] undertaking that should utilize *contextually targeted* solutions while leveraging a *broader network* of support. Policy advocacy for internet policy development requires communication, cooperation, and action across multiple platforms and venues, including at the local, regional, and international levels. Strategically engaging with various actors within the advocacy community is an important aspect of successful advocacy work. Referencing international standards for human rights in internet policy can strengthen national advocacy efforts, as was done by a coalition of civil society groups and some private technology companies in Burma during a push for stronger data protection legislation in 2016.[95] Building coalitions with international organizations can also amplify media coverage of national and regional campaigns, putting pressure on government actors to address targeted issues and align with international internet principles.[96] Those engaged in internet policy development should also "help local experts and core network organizations work with one another" to expand the number of engaged stakeholders and strengthen advocacy efforts.[97] Critically, "building broad civil society coalitions" that link together numerous individual actors increases the likelihood of successfully impacting internet policy in the long-term.[98] This emphasis on creating *communities* that collectively engage in internet policymaking processes is seen across the literature.

Meaningful engagement in internet policy development should be understood as a multi-step concept. Rather than defining "successful" advocacy as the wholesale adoption of a recommended policy, policy advocacy and policy development should be seen as a broader "enlightenment process."[99] This broader advocacy and policy development process involves three distinct yet overlapping approaches:

- developing technical and organizational capacity;
- broadening policy horizons to clearly frame the problem and possible policy solutions; and
- generating a tangible impact through change in policy.[100]

Similarly, a set of nine case studies published by the Center for International Media Assistance (CIMA) identifies four common strategies used by civil society actors to engage in internet policy making processes, particularly when it comes to DDoS attacks. These four engagement strategies include: awareness-raising, nonviolent direct action, regional and international coalition-building, and rights advocacy litigation.[101] Advocacy via nonviolent engagement was utilized recently in Singapore and Australia, for example, where

[94] Internet Society. (2016). Internet Governance – Why the Multistakeholder Approach Works. Internet Society. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

[95] Hynes, Casey. (2016). Digital Rights Must Become A Top Priority In Myanmar's Connectivity Revolution. Forbes. https://www.forbes.com/sites/chynes/2016/12/21/digital-rights-must-become-a-top-priority-in-myanmars-connectivity-revolution/?sh=659f29d02267. See also Oh, Sarah. (2017). Advocating for Openness: Nine Ways Civil Society Groups Have Mobilized to Defend Internet Freedom. CIMA. https://www.cima.ned.org/publication/advocating-openness-nine-ways-civil-society-groups-mobilized-defend-internet-freedom/

[96] Oh, Sarah. (2017). Advocating for Openness: Nine Ways Civil Society Groups Have Mobilized to Defend Internet Freedom. CIMA. https://www.cima.ned.org/publication/advocating-openness-nine-ways-civil-society-groups-mobilized-defend-internet-freedom/

[97] Zuckerman, E. et al. (2010). Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites. The Berkman Center for Internet & Society at Harvard University. https://www.opensocietyfoundations.org/uploads/88c8cc50-b839-4250-a2ea-f045940565b8/Political-DDoS-20110106.pdf

[98] Oh, Sarah. (2017). Advocating for Openness: Nine Ways Civil Society Groups Have Mobilized to Defend Internet Freedom. CIMA. https://www.cima.ned.org/publication/advocating-openness-nine-ways-civil-society-groups-mobilized-defend-internet-freedom/

[99] Carden, Fred. (2009). Knowledge to Policy: Making the most of development research. International Development Research Center. https://www.idrc.ca/sites/default/files/openebooks/417-8/index.html

[100] Young, E. & Quinn, L. (2012). Making Research Evidence Matter: A guide to policy advocacy in transition countries. International Centre for Policy Advocacy. https://advocacyguide.icpolicyadvocacy.org/236-what-is-the-goal-of-policy-advocacy#fn:236

[101] Oh, Sarah. (2017). Advocating for Openness: Nine Ways Civil Society Groups Have Mobilized to Defend Internet Freedom. CIMA. https://www.cima.ned.org/publication/advocating-openness-nine-ways-civil-society-groups-mobilized-defend-internet-freedom/

public outcry cultivated in response to the inappropriate use of data collected from COVID-related smartphone applications resulted in policy changes that govern data use by law enforcement bodies.[102]

Linked to this expansive understanding of policy advocacy is the importance of building the capacity of local actors. Indeed, capacity development is seen among advocacy groups as a central element of the policy development process, providing civil society and individuals the core knowledge to not only get involved in policymaking but to actually create change. There exist a variety of informational sources to support self-guided capacity development to enhance basic understanding of internet policy issues, recommended standards, and advocacy areas—such as, for example, training materials developed by the American Bar Association with funding from the U.S. DoS.[103] However, implementing the information and recommendations found in training materials is not always straightforward and can be impacted by the unique contextual realities that local actors face. Indeed, a 2017 survey of 79 organizations engaged in digital freedom advocacy around the world revealed that many organizations perceive that "research in the field is driven by the priorities of Western countries."[104] This connects back to the importance of identifying and supporting contextually targeted knowledge generation and solutions, not only those issues identified by outsiders, as important. Beyond identifying and understanding priority issue areas, organizations must also have the capacity to engage meaningfully in policy advocacy activities that are pertinent to their context and their topical needs. Organizational capacity, therefore, is often seen as a fundamental challenge to civil society being able to engage in standard-setting and policy making processes concerning internet governance and human rights on the internet.[105]

Some of the best practices and recommendations concerning policy advocacy and human rights in internet policy, as found in the available literature, are reflected in the approaches utilized by the sampled programs within this line of effort. Those programs include Policy Advocacy Project A to deliver financial support, technical and operational skills trainings, partnerships, and apprenticeship programs to enhance the capacity and sustainability of grassroots internet freedom advocacy. The second program comprised a grant to develop and implement an interdisciplinary, competitive event (aka Policy Advocacy Project B) in each target country where CSOs develop innovative ideas to address digital/economy challenges. The winner of each Policy Advocacy Project B event attended a project development bootcamp to turn their ideas into viable potential programs. Top programs were then selected to receive seed funding. The approaches of these two programs differ slightly—the first delivered financial, technical, and operational support directly to CSOs while the second created an environment where CSOs could develop unique technical solutions while receiving operational guidance. Although distinct, both approaches reflect key components of the best practices identified in the literature review—namely, a focus on capacity development, contextually tailored solutions, and a network approach.

Legal Advocacy

Legal advocacy comprises a suite of diverse engagement strategies to promote the use of the law as a means of redress. Civil society is an effective and important actor in the legal advocacy space, for internet freedom issues and other sectors, through its provision of vertical accountability. "Vertical accountability refers to power relations between the State and its citizens" and is distinct from horizontal accountability, which is the

[102] Shahbaz, A. & Funk, A. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf
[103] American Bar Association. (n.d.). Internet Freedom (Past Program). https://www.americanbar.org/advocacy/rule_of_law/where_we_work/europe_eurasia/internet-freedom/
[104] Remensperger, John & Schwartz-Henderson, Laura & Cendic, Kristina. (2018). Using Research in Digital Rights Advocacy: Understanding the Research Needs of the Internet Freedom Community. Internet Policy Observatory. https://www.asc.upenn.edu/sites/default/files/2021-02/using-research-in-digital-rights-advocacy-internet-policy-observatory.pdf
[105] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23

system of checks and balances within the State structure itself.[106] By engaging in vertical accountability, civil society actors can in turn influence public priorities and advocate for those issues in front of the State. A variety of legal advocacy approaches have been documented.

Rights advocacy litigation is a common form of legal advocacy. Rights advocacy litigation, also known as impact litigation, involves selecting and bringing specific cases to court that have precedent-setting power and "will pave the way for further litigation" as well as legislative change.[107] Civil society can and does play an active role in rights advocacy litigation in the form of bringing cases to court, appearing in proceedings as amicus curiae, and preparing and/or signing amicus briefs.[108] Rights advocacy litigation is also a powerful awareness-raising tool. Even if the case is lost, rights advocacy litigation can help to bolster the public's awareness and prioritization of the issue.[109] Legal advocacy thus comprises an important communications element, and civil society plays a key role in reaching technical stakeholders and the general public. They lead communication campaigns to inform the public of illiberal laws and generate grassroots support to challenge those laws and policies.[110] This can often be taken further in the form of organizing protests and demonstrations, promoting boycotts, and undertaking "naming and shaming" campaigns.[111] While it is difficult to measure the effects of civil society's legal advocacy work, particularly on the communications front, it is argued by some that these types of activities are one of "the elements that convinced [others] … to act bravely."[112]

In authoritarian or authoritarian-leaning countries, the use of courts on issues relating to internet freedom primarily centers on the efforts of governments to regulate technology companies, pursue targeted individuals, and strengthen repressive policies relating to internet access and human rights-related issues.[113] China, India, Turkey, Indonesia, and Russia, among others, have recently enacted laws that strengthen the state's ability to subject tech companies and their employees to judicial fines and criminal charges for failure to comply with broad and vaguely defined internet content laws (or specific laws that directly infringe on human rights and democratic principles); these policies, and the threat/use of the courts to promote adherence, "bring the private sector further under the authority of the state in a bid to more effectively stamp out dissent, conduct blanket surveillance, and disseminate propaganda."[114] In these cases, support to the

[106] Tsampi, Aikaterini. (2021). The Role of Civil Society in Monitoring the Executive in the Case-Law of the European Court of Human Rights: Recasting the Rule of Law. *Utrecht Law Review*, 17(2). http://doi.org/10.36633/ulr.671

[107] Bateman, J. (2021). Why Climate Lawsuits are Surging. BBC. https://www.bbc.com/future/article/20211207-the-legal-battle-against-climate-change

[108] American Civil Liberties Union. (n.d.). Important Internet Free Speech Litigation. https://www.aclu.org/other/important-internet-free-speech-litigation. See also American Civil Liberties Union. (n.d.). Internet Speech. https://www.aclu.org/issues/free-speech/internet-speech; Association for Civil Rights. (2021). ADC intervenes as amicus curiae in Supreme Court hearing in Denegri v. Google case. https://adc.org.ar/en/2022/03/18/adc-intervenes-as-amicus-curiae-in-supreme-court-hearing-in-denegri-v-google-case/

[109] Amnesty International. (n.d.). Strategic Litigation. https://www.amnesty.org/en/strategic-litigation/

[110] Bojarski, L. (2021). Civil Society Organizations for and with the Courts and Judges—Struggle for the Rule of Law and Judicial Independence: The Case of Poland 1976–2020. German Law Journal (Vol. 22, Special Issue 7). https://www.cambridge.org/core/journals/german-law-journal/article/civil-society-organizations-for-and-with-the-courts-and-judgesstruggle-for-the-rule-of-law-and-judicial-independence-the-case-of-poland-19762020/78B99D55550E5668F9363F2A9FA827EB

[111] Bateman, J. (2021). Why Climate Lawsuits are Surging. BBC. https://www.bbc.com/future/article/20211207-the-legal-battle-against-climate-change

[112] Bojarski, L. (2021). Civil Society Organizations for and with the Courts and Judges—Struggle for the Rule of Law and Judicial Independence: The Case of Poland 1976–2020. German Law Journal (Vol. 22, Special Issue 7). https://www.cambridge.org/core/journals/german-law-journal/article/civil-society-organizations-for-and-with-the-courts-and-judgesstruggle-for-the-rule-of-law-and-judicial-independence-the-case-of-poland-19762020/78B99D55550E5668F9363F2A9FA827EB

[113] Shahbaz, A. & Funk, A. (2021). *Freedom on the Net 2021: The Global Drive to Control Big Tech*. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

[114] Shahbaz, A. & Funk, A. (2021). *Freedom on the Net 2021: The Global Drive to Control Big Tech*. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

defense strategy is a crucial tool to protect internet freedom. In countries where rule of law is stronger, legal advocacy is a critical method to combat repressive application of policies or to challenge the constitutionality of laws themselves. Thus, in addition to supporting defense strategies, donors have supported proactive litigation led by civil society.

To reach relevant technical stakeholders, civil society also organizes important seminars on internet freedom issues related to upcoming or ongoing litigation efforts.[115] Civil society can also help to generate archives of legal developments, case law, and related information across jurisdictions. However, such repositories are currently lacking; a recent survey of organizations engaged in digital rights advocacy work around the world revealed the desire among these organizations for "the need for comprehensive databases aggregating legislation and case law across a variety of jurisdictions."[116]

Civil society additionally contributes to the broader legal advocacy environment by developing and/or delivering specialized training to, for example, lawyers or judges who are interested in supporting internet freedom-related casework.[117] The ramifications of rapidly evolving technology can swiftly outpace the law. Activists engaging in diverse and emerging internet-related issue areas report the challenge of "lawyers, often old white men, who told us our ideas were not possible because of the law."[118] This exemplifies the need for a new generation of tech savvy lawyers, that - preferably - have community ties, and thus better understanding of the policy impact. Delivering training to lawyers and judges provides the necessary technical capacity building while also contributing to an environment where legal experts are able and willing to potentially advocate for important internet freedom issues.

The evaluation sample contains two programs that sought to empower civil society to challenge illiberal laws and policies: (1) Policy Advocacy Project C and (2) Policy Advocacy Project D. Both programs included capacity building programming alongside the generation and dissemination of technical content to support legal advocacy—all critical aspects of legal advocacy identified in the available literature. Of interest, both programs took a cross-border approach to capacity building and learning and thus reflected one of the key tenets found in advocacy for human rights in internet policy, discussed above. Regional summits (in the case of Policy Advocacy Project C) and international study trips (in the case of Policy Advocacy Project D) connected targeted stakeholders with a broader group of peers to enhance the discussion of best practices and promote learning. Regarding the generation and dissemination of technical content, both programs developed educational materials and guidance documents tailored to the implementation contexts. Policy Advocacy Project D directly supported civil society in challenging illiberal laws and policies as it sought to provide subject matter expertise to stakeholders in approximately 100 court cases related to internet censorship. Reflective analysis from those 100 court cases is to be prepared and shared with the general public.

[115] Association for Civil Rights. (2022). ADC and UCLA hold an event on facial recognition in Argentina. https://adc.org.ar/en/2022/03/09/adc-and-ucla-hold-an-event-on-facial-recognition-in-argentina/

[116] Remensperger, John & Schwartz-Henderson, Laura & Cendic, Kristina. (2018). Using Research in Digital Rights Advocacy: Understanding the Research Needs of the Internet Freedom Community. Internet Policy Observatory. https://www.asc.upenn.edu/sites/default/files/2021-02/using-research-in-digital-rights-advocacy-internet-policy-observatory.pdf

[117] American Bar Association. (n.d.). Internet Freedom (Past Program). https://www.americanbar.org/advocacy/rule_of_law/where_we_work/europe_eurasia/internet-freedom/. See also Green, Natalie & Rossini, Carolina. (2015). Open Internet Course. Public Knowledge. https://publicknowledge.org/open-internet-course/

[118] Bateman, J. (2021). Why Climate Lawsuits are Surging. BBC. https://www.bbc.com/future/article/20211207-the-legal-battle-against-climate-change

Research

Global Rankings

Besides providing a normative basis for declaring a certain set of conditions as illegal, human rights are able to inform debates and empower CSOs and activists alike through a set of analytic tools for scanning and rating actions of powerful institutions, including governments and technology companies. [119] Research in digital rights advocacy is needed because accurate and systematically collected information is very helpful to persuade policymakers, communicate with stakeholders, convince funders to support a certain approach, educate journalists and impact public opinion.[120]

In this context, the development of "human rights indicators"' has proven to be a useful tactic. Indicators support the measurement and assessment of, for example, the extent to which rights are being fulfilled or enjoyed in a given situation.[121] Indicators are, however, hard to develop. They need time, funding, and expert knowledge so their methodology and results are trustworthy and can be used to inform advocacy efforts. This is especially true for digital rights-related advocacy, where methods for investigating the internet's policy effects, internet users' behavior, and corporate decision-making are often highly technical, sensitive, and ever-changing.[122] It can also be hard for policy makers and the public at large to understand granular information on these issues.

Few organizations have the technical and funding ability to develop such assessments. According to a 2018 report by the Internet Policy Observatory, which surveyed 79 organizations in the digital rights advocacy field, interviewees cited gaps in research methods expertise and perceived a need for them to have training both in newer technical methods such as social network analysis, network measurement and in legal research. Programs that assess rights compliance by both countries and technology companies, providing stakeholders with reliable indicators-based information in a user-friendly way, notably through indexes and rankings, are crucial and have been culturally accepted as generally reliable and legitimate. In digital rights research, the indexes and rankings that have emerged over the years usually rely on composite information, with the general purpose of providing both individual assessments and allowing for a comparative analysis of the actors they map with respect to rights such as privacy and freedom of expression.[123] "These rankings are effective at changing the behavior of the actors being ranked, be they countries, companies, or other entities."[124] Exposing the specific areas where a given company is lacking will inform company-oriented advocacy strategies by advocates, clients and even board members. Having access to the indicators of a given company's compliance with human rights can be a powerful negotiation and advocacy for change tool, especially if the company's result in comparison is unfavorable.[125] It will also support the company itself in improving processes and conduct.

[119] Green, Maria. (2001). What We Talk About When We Talk About Indicators: Current Approaches to Human Rights Measurement. Human Rights Quarterly 23. https://www.jstor.org/stable/4489371?seq=1.

[120] Remensperger, John & Schwartz-Henderson, Laura & Cendic, Kristina. (2018). Using Research in Digital Rights Advocacy: Understanding the Research Needs of the Internet Freedom Community. Internet Policy Observatory. https://www.asc.upenn.edu/sites/default/files/2021-02/using-research-in-digital-rights-advocacy-internet-policy-observatory.pdf

[121] Green, Maria. (2001). What We Talk About When We Talk About Indicators: Current Approaches to Human Rights Measurement. Human Rights Quarterly 23. https://www.jstor.org/stable/4489371?seq=1.

[122] Remensperger, John & Schwartz-Henderson, Laura & Cendic, Kristina. (2018). Using Research in Digital Rights Advocacy: Understanding the Research Needs of the Internet Freedom Community. Internet Policy Observatory. https://www.asc.upenn.edu/sites/default/files/2021-02/using-research-in-digital-rights-advocacy-internet-policy-observatory.pdf

[123] Maréchal, Nathalie. (2015). Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate. International Journal of Communication 9. https://ijoc.org/index.php/ijoc/article/viewFile/3330/1494.

[124] Ibid.

[125] Ibid.

A strategy that many companies have adopted, especially since 2010, to improve their corporate social responsibility practices is the publication of transparency reports, in which they disclose "aggregate data about government requests for user data, government demands to remove content, and intellectual property-related takedowns. [Such], transparency reports offer companies a public-facing opportunity to showcase their values and commitments to protecting user rights."[126] These transparency reports are not government- or industry-mandated, but some organizations, such as the Global Network Initiative (GNI), have been prominent in promoting this trend. GNI encourages companies to improve their practices and "identify circumstances where freedom of expression and privacy may be jeopardized" through methods such as human rights due diligence and human rights impact assessments. [127]

Providing measurable and clear evidence is a valuable exercise to inform civil society, decision-makers and policymakers, and the public at large. This accessible representation of complex information is useful both to provide evidence-based information for the action of digital rights activists to hold governments accountable and to empower both public and private organizations as well as investors to distinguish between technology companies who pay lip service to corporate social responsibility and those who actually respect and promotes digital rights.[128]

In the scope of the Internet Freedom Portfolio, Research Project A aligns with this target by producing the a ranking of the world's most powerful digital platforms and telecommunication companies on their disclosed commitments and policies affecting freedom of expression and privacy.[129] In Research Project A's words, "by benchmarking and ranking them against standards that set high but achievable goals for corporate transparency and rights-respecting policies, [Research Project A] gives companies an incentive to improve their policies and practices over time."[130] The Research Project A, now in its fifth iteration, seeks to change corporate behavior in the technology sector for its better alignment.[131,132]

Also focused on ranking countries, the Internet Freedom Portfolio-funded Research Project B investigates whether governments are complying with digital rights, and in addition to publishing country-studies, produces a rank. Specifically, Research Project B crafts a "ranked, country-by-country assessment of online freedom, a global overview of the latest developments, as well as in-depth country reports."[133] Research Project B also trains activists, advocates and scholars in many countries on digital rights research, since local groups often lack expertise in systematically monitoring developments relevant to internet freedom[134]. By taking this approach, Research Project B aims to help local digital rights activists, bloggers, and researchers to better understand technical and legal methods of internet censorship and enables them to track developments in their countries, ultimately gaining skills to better hold their governments accountable.[135]

[126] New America. (n.d.). Case Study #3: Transparency Reporting. New America, Getting Internet Companies To Do The Right Thing. https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/.

[127] Global Network Initiative. (2020). Increasing Transparency on Human Rights Due Diligence and Impact Assessments by GNI Company Members. Global Network Initiative. https://globalnetworkinitiative.org/increasing-transparency-on-human-rights-due-diligence-and-impact-assessments-by-gni-company-members/

[128] Maréchal, Nathalie. (2015). Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate. International Journal of Communication 9. https://ijoc.org/index.php/ijoc/article/viewFile/3330/1494.

[129] Research Project A. (2021). Final Evaluation.

[130] Research Project A. (n.d.). Who We Are.

[131] Research Project A. (2021). Final Evaluation.

[132] Research Project A. (n.d.). Methodology Development.

[133] Research Project B. (2021). Document on file with evaluation team.

[134] Ibid.

[135] Ibid.

SAFEGUARDING INTERNET FREEDOMS

Focusing on EQ3, this section aims to provide a solid understanding of the existing technical evidence pertaining to the most common and best practices with respect to safeguards.

3) EQ3 – How have DRL's current safeguards been successful in minimizing the use of Internet Freedom-funded technologies developed within the Technology Development Pillar for illicit purposes, considering the risks and benefits of those safeguards to the Internet Freedom Program's ability to meet the objectives, goals, and values in the Internet Freedom Strategic Framework?

   – Which safeguards have not been effective among these?

   – What are other effective safeguards that the DRL internet freedom team should consider utilizing to minimize internet freedom-funded technologies for illicit purposes?

International Standards and Best Practices

At the core of the Internet Freedom Portfolio lies the aim "to protect the open, interoperable, secure, and reliable internet by promoting fundamental freedoms, human rights, and the free flow of information online through integrated support to civil society for technology, digital safety, policy and advocacy, and applied research programs."[136] While promoting these values and capabilities, the Internet Freedom Portfolio's Technology Development pillar supports 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."[137] On the one hand, these tools 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 defend human rights and fight for democratic values, and on the other hand, there is a constant concern that these same tools could potentially be used for illicit purposes.

This situation presents the possible trade-offs of any technology – as technology is in itself neutral, it can be used for good or bad by those who develop it, control it, access it, and/or use it. Specifically, while helping to promote and provide "safe, reliable, and anonymous Internet access to people who would otherwise be censored, filtered, or punished for communicating electronically,"[138] anti-censorship and privacy protecting technology could also help certain actors "to conceal or commit illegal activity"[139] and even present a threat "to other aspects of … national security."[140] This trade-off is anchored in an extensive debate on the

[136] US Department of State, Bureau of Democracy, Human Rights, and Labor. (2021) DRL FY22 Internet Freedom Annual Program Statement. US Department of State.
[137] United States Congress. (2020). Consolidated Appropriations Act, Section 705. United States Government
[138] Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva. (2015). "Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals." RAND Corporation. https://www.rand.org/pubs/research_reports/RR1151.html.
[139] Ibid.
[140] 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

importance and role of anonymity versus attribution or, simply put, the apparent clash between Internet Freedom versus [Cyber and/or National] security.[141]

On the one hand, the exercise of internet freedoms requires anonymity and privacy to protect human rights activists and defenders of democratic values defenders across the world. Anonymity is essential to protect these users from "political or economic retribution, harassment, or even threats to their lives."[142] Furthermore, "the right to anonymous free speech is protected by the First Amendment"[143] and in Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[144] On the other hand, cyber security entails online transparency and attribution, among other features, since they are key to identifying and prosecuting cybercriminals. In this sense, cyber security aims to make "geo-location, intelligence analysis and impact assessment – who did it, from where, why and what was the result" more manageable.[145] Considering such risks, implementing safeguards that can mitigate the risk of using such tools for illicit purposes is of high importance to balance the trade off to the side of the "good."

A core principle, foundational to mitigate the illicit use of technology designed to circumvent censorship to publish, post, and share information or to provide access to information online and offer secure communications while protecting anonymity is to embed the development of such tools within a "human-rights-by-design" principle. The **"human-rights-by-design"** principle entails having companies and tech developers "commit to designing tools, technologies, and services to respect human rights by default, rather than permit abuse or exploitation as part of their business model."[146] A human rights-based approach is strengthened by the following five safeguards or implementation principles:[147,148]

1) **Participation:** in the decision-making process when it comes to the enjoyment of rights.
2) **Accountability:** of law enforcement to ensure one's ability to exercise their rights.
3) **Non-discrimination:** prohibition on any sort of discrimination.
4) **Empowerment:** entitlement to claim ones' rights.
5) **Legality:** technology should be in line with human rights.

The commitment to a human rights-based approach encompasses actions to "prevent filtering companies from designing their technology with features that enable large-scale, indiscriminate, or inherently disproportionate censorship capabilities" and having "algorithms incorporated into the design of communications and storage platforms" that "could account for human rights considerations in addition to business objectives."[149] Ultimately, this suggests that tools developed within a human rights-based approach,

[141] 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

[142] Electronic Frontier Foundation. (n.d.). Anonymity. Electronic Frontier Foundation. https://www.eff.org/issues/anonymity

[143] Ibid.

[144] Association for Progressive Communications. (2015). The right to freedom of expression and the use of encryption and anonymity in digital communications. Association for Progressive Communications. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/AssociationForProgressiveCommunication.pdf

[145] 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

[146] Penney, Jonathan and Sarah McKune, Lex Gill, Ronald J. Deibert. (2018). Advancing Human-Rights-By-Design In The Dual-Use Technology Industry. Columbia Journal of International Affairs. https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry

[147] Ochom, Jonathan. (2022). The Case For A Human Rights-Based Approach To Technology. Human Rights Pulse. https://www.humanrightspulse.com/mastercontentblog/the-case-for-a-human-rights-based-approach-to-technology

[148] European Network of National Human Rights Initiative. (n.d.). Human Rights-Based Approach. ENNHRI. https://ennhri.org/about-nhris/human-rights-based-approach/

[149] Penney, Jonathon, Sarah Mckune, Lex Gill, and Ronald J. Deibert. (2018). Advancing Human-Rights-by-Design in the Dual-Use Technology Industry. Journal of International Affairs. Colombia School of International and Public Affairs. https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry

with the goal to protect and promote human rights – should have less potential to be used for illicit purposes than comparable technologies designed without a human rights-based approach. For example, "mainstream services like WhatsApp and iMessage" have historically, more commonly been used by criminals than their comparable technologies "because they are cheap, easy to access and allow [criminals] to communicate with a wide audience" with ease for their illicit products and activities.[150]

Notably, research indicates that criminals – in an attempt to "remain unknown except to the small number of people who use" a given technology and to avoid the security vulnerability of the most popular services – are shifting their attention to services that provided "next-level security" and encryption.[151] Technologies, such as Phantom Secure, EncroChat and Sky Global, are designed to provide targeted services solving specific access limitations with a commercial focus, rather than focusing on a human-right issue, lending itself to becoming more susceptible to illicit uses and consequently, to law enforcement.

Safeguarding internet freedoms and mitigating the potential of a given technology to be used for illicit purposes begins at the design and development stage. The intent or purpose to which a tool is built and the level to which it embeds human rights in its design is a foundational step towards mitigating the illicit use of a technology. As discussed below, DRL/GP's Internet Freedom Portfolio and its stated goals to develop and scale technologies which provide (1) unrestricted access to the free and open internet and (2) ensure surveillance-free communications to protect one's anonymity – are aligned with the promotion of human right. In addition, DRL/GP's commitment to a human rights-by design approach, suggests that these technologies should offer solutions that are not necessarily the most appealing or most easily accessible to criminals and thus, acts of cybercrime.

DRL/GP Internet Freedom Safeguards

According to DRL's established "illicit use mitigation strategy" and its definition of safeguards to prevent illicit use of tools[152] technologies developed and/or funded by the Internet Freedom Portfolio are to ensure the application of a human rights frameworks to programming (e.g., privacy for design, security by design, etc.). DRL's "illicit use mitigation strategy, in alignment with best practices in Internet Freedom safeguards as described above, is built on three key components. These include:[153]

1. **Application of a human rights framework to Internet freedom programming**, which includes requiring software development consistent with the human rights use case, and the development of human rights and technology community standards.

2. **Application of proposal and project review controls**, to review and assess the risk of illicit use throughout the proposal review and program implementation cycle.

3. **Evaluation, on a periodic basis, of illicit misuse mitigation strategy**, by means of external reports such as RAND Corporation's.

[150] West, Ben. (2021). Crime and Technology, Part 1: Secure Communication Platforms. Stratfor. https://worldview.stratfor.com/article/crime-and-technology-part-i-secure-communication-platforms?utm_source=pocket_mylist
[151] Ibid.
[152] Safeguards to prevent illicit use of tools is defined as a strategy – technical or behavioral – for preventing or making less likely the illicit use of IF-funded tools. It includes the application of a human rights frameworks to programming (e.g., privacy for design, security by design, etc.) and thus a focus on (1) identifiable human rights organizations 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.
[153] Bureau of Democracy, Human Rights, and Labor, Office of Global Programs – Internet Freedom. "Summary of DRL Internet Freedom Illicit Use Mitigation Strategy". February 9 Final.

Between 2014 – 2015, DRL contracted RAND to develop a methodology to assess the effectiveness of the established Internet Freedom Portfolio safeguards and the level of its effectiveness in preventing illicit use of its technologies. The methodology, as outlined in the 2015 Rand report *Internet Freedom Software and Illicit Activity – Supporting Human Rights Without Enabling Criminals* assesses the potential for illicit-use of Internet Freedom Portfolio-funded technologies by answering three key questions:

- Does it solve a criminal's communication problem?
- Does it provide a material advantage to criminals?
- Is the tool reasonably accessible to criminals?

As a result of this effort, RAND concluded that the Internet Freedom Portfolio programs did not "materially support or improve the capabilities of criminals and their activities."[154] It also concluded that Internet Freedom Portfolio-funded technologies had the potential to "provide a critical service to its intended audience – human rights activists and other at-risk groups across the world," by offering secure means of communication, enhancing their personal safety and allowing them to continue working.[155] Moreover, as part of this assessment, RAND identified several additional safeguards developed and implemented by the participating grantees. These included:

- **Limited availability:** Availability of the technology developed to a limited group of known individuals who could be vetted (e.g., end users could be vetted by providers and had to support human rights activities).
- **Limited training availability:** Offering only in-person training is also considered an availability deterrent.
- **Lawful investigation:** It should be possible to submit the technology developed to lawful investigation, which is assumed to provide a strong deterrent against criminal use.
- **It is not the best tool to meet a criminal's needs:** Existing alternatives that are non-DRL funded and could better meet the needs of illicit users could be considered a form of safeguard.
- **Paid service with a high cost:** Services that are paid or have a high cost are also generally seen as deterrents against criminal use.

Finally, as part of RAND's assessment, the team recommended a set of additional safeguards to further prevent the illicit use of the Internet Freedom Portfolio-funded technologies. These include:

- Encourage **broader localization, digital safety training, and awareness efforts** by more grantees in more countries around the world.
- Request that each grantee **documents safeguards, designs, assumptions,** and other factors that would limit, restrict, or deter use of its technologies by criminals. Document any illicit use of the tool.
- Develop technologies that are of **greater interest to netizens** and have less potential to interest criminals.
- **Undertake and invest in research**:
  - to better understand the differences in uses and preferences between netizen and criminals.
  - to better understand preferences and constraints, uncovering a better combination and application of safeguards to implement across the portfolio.

[154] Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva. (2015). Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals. RAND Corporation. https://www.jstor.org/stable/10.7249/j.ctt17mvhd1

[155] Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva. (2015). Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals. RAND Corporation. https://www.jstor.org/stable/10.7249/j.ctt17mvhd1.

– to examine and quantify network behavior to understand the "kinds of traffic (legal and illicit) that pass-through privacy and security tools in general"[156] as a way to inform the policy debate concerning the illicit use of Internet Freedom tools.

Although the specific program documentation reviewed to date – including Technology Project B, Technology Project A, Technology Project C, and Technology Project D – do not explicitly mention which safeguards were specifically adopted, the available reports do suggest certain safeguards were put in place. These are summarized in the table below.

Table 1. Application of DRL/GP Internet Freedom Safeguards

DRL/GP Internet Freedom Illicit Use Mitigation Strategy and Safeguards	Technology Project B	Technology Project A	Technology Project C	Technology Project D
Illicit Use Mitigation Strategy	🟦	🟦	🟦	🟦
Application of human rights framework to Internet freedom programming		🟦	🟦	
Application of proposal and project review controls				
Evaluation, on a periodic basis, of illicit misuse mitigation strategy		🟦	🟦	
Additional Safeguards				
Limited availability	🟦	🟦	🟦	
Limited training availability			🟦	
Lawful investigation				🟦
Doesn't fit a criminals' needs				
Paid service with high cost				
Recommended Safeguards				
Broader localization, digital safety training, and awareness efforts				
Documentation of safeguards, designs, and assumptions				
Greater interest to netizens				
Undertake and invest in research				

The evaluation team will build on the information presented in the table above through additional desk research, key informant interviews, focus group discussions, and an online survey to understand more fully which safeguards were adhered to across the selected programs.

[156] Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva. (2015). Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals. RAND Corporation. https://www.jstor.org/stable/10.7249/j.ctt17mvhd1

REFERENCES

Access Now. (2021). “#KeepItOn: Fighting Internet Shutdowns around the World.” https://www.accessnow.org/keepiton/.

Access Now. (2016). “Ways to Circumvent the Internet Shutdown in the Democratic Republic of Congo.” https://www.accessnow.org/ways-circumvent-internet-shutdown-democratic-republic-congo/.

American Bar Association. (n.d.). Internet Freedom (Past Program). https://www.americanbar.org/advocacy/rule_of_law/where_we_work/europe_eurasia/internet-freedom/

American Civil Liberties Union. (n.d.). Important Internet Free Speech Litigation. https://www.aclu.org/other/important-internet-free-speech-litigation

American Civil Liberties Union. (n.d.). Internet Speech. https://www.aclu.org/issues/free-speech/internet-speech

Ammarah Cheema, Moeenuddin Tariq, Adnan Hafiz, Muhammad Murad Khan, Fahad Ahmad, Muhammad Anwar, "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review", Security and Communication Networks, vol. 2022, Article ID 8379532, 15 pages, 2022. https://doi.org/10.1155/2022/8379532

Amnesty International. (n.d.). Strategic Litigation. https://www.amnesty.org/en/strategic-litigation/

ARTICLE 19. (2018). “Navigating the ITU: Charting the Paths Forward for Civil Society.” https://www.article19.org/resources/navigating-itu-charting-paths-forward-civil-society/.

Association for Civil Rights. (2021). ADC intervenes as amicus curiae in Supreme Court hearing in Denegri v. Google case. https://adc.org.ar/en/2022/03/18/adc-intervenes-as-amicus-curiae-in-supreme-court-hearing-in-denegri-v-google-case/

Association for Civil Rights. (2022). ADC and UCLA hold an event on facial recognition in Argentina. https://adc.org.ar/en/2022/03/09/adc-and-ucla-hold-an-event-on-facial-recognition-in-argentina/

Association for Progressive Communications. (2015). The right to freedom of expression and the use of encryption and anonymity in digital communications. Association for Progressive Communications. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/AssociationForProgressiveCommunication.pdf

Barabas, Chelsea and Neha Narula, Ethan Zuckerman. (2017). “Back to the Future: The Decentralized Web.” https://dci.mit.edu/research/the-decentralized-web.

Bateman, J. (2021). Why Climate Lawsuits are Surging. BBC. https://www.bbc.com/future/article/20211207-the-legal-battle-against-climate-change

Bojarski, L. (2021). Civil Society Organizations for and with the Courts and Judges—Struggle for the Rule of Law and Judicial Independence: The Case of Poland 1976–2020. German Law Journal (Vol. 22, Special Issue 7). https://www.cambridge.org/core/journals/german-law-journal/article/civil-society-organizations-for-and-with-the-courts-and-judgesstruggle-for-the-rule-of-law-and-judicial-independence-the-case-of-poland-19762020/78B99D55550E5668F9363F2A9FA827EB

Bureau of Democracy, Human Rights, and Labor, Office of Global Programs – Internet Freedom. “Summary of DRL Internet Freedom Illicit Use Mitigation Strategy”. February 9 Final.

Carden, Fred. (2009). Knowledge to Policy: Making the most of development research. International Development Research Center. https://www.idrc.ca/sites/default/files/openebooks/417-8/index.html

Carothers, Saskia Brechenmacher, Thomas. "Defending Civic Space: Is the International Community Stuck?" Carnegie Endowment for International Peace. Accessed May 25, 2022. https://carnegieendowment.org/2019/10/22/defending-civic-space-is-international-community-stuck-pub-80110.

Cavoukian, Ann. (2011). Privacy by Design: The 7 Foundational Principles. Privacy by Design. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

Clinton, Hillary. (2011). Internet Rights & Wrongs: Choices and Challenges in a Networked World. American Rhetoric Online. https://www.americanrhetoric.com/speeches/hillaryclintoninternetpolicyspeechgw.htm

Clinton, Hillary Rodham. (2010). Remarks on Internet Freedom. US Department of State. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Collett, Robert, Nayia Barmpaliou, Patryk Pawla. (2021). International Cyber Capacity Building: Global Trends and Scenarios. European Commission. https://www.iss.europa.eu/content/international-cyber-capacity-building-global-trends-and-scenarios

Counterpart. (2017). "Civil Society & Government Unite For a Free and Open Internet." Accessed May 25, 2022. https://www.counterpart.org/stories/civil-society-gov-advance-free-and-open-internet/.

Counterpart. (n.d.). "How We Achieve Change." https://www.counterpart.org/our-work/how/

Committee to Protect Journalists. (2022). Digital Safety Kit. https://cpj.org/2019/07/digital-safety-kit-journalists/

Congressional Research Service. (2016). Promoting Global Internet Freedom: Government and Industry Initiatives. CRS Report R41837.

Conversation, The. (2021). "How 'Human Rights by Design' Can Save Us from AI Misuse." TNW | Neural. https://thenextweb.com/news/how-human-rights-by-design-can-save-us-from-ai-misuse-syndication

Court, Julius, Enrique Mendizabal, David Osborne, and John Young. (2006). "Policy Engagement: How Civil Society Can Be More Effective." ODI: Think change. https://odi.org/en/publications/policy-engagement-how-civil-society-can-be-more-effective/

Digital Safety Project B. (2019). Final Project Report. On file with evaluation team.

Dutta, Saurabh. (2017). "Striking a Balance between Usability and Cyber-Security in IoT Devices." Thesis, Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/113508.

Electronic Frontier Foundation. (n.d.). Anonymity. Electronic Frontier Foundation. https://www.eff.org/issues/anonymity

Engler, Alex. (2022). The Declaration for the Future of the Internet is for wavering democracies, not China and Russia. Brookings. https://www.brookings.edu/blog/techtank/2022/05/09/the-declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/

European Network of National Human Rights Initiative. (n.d.). Human Rights-Based Approach. ENNHRI. https://ennhri.org/about-nhris/human-rights-based-approach/

Feldstein, Steven. (2022). "Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?" Carnegie Endowment for International Peace.

https://carnegieendowment.org/2022/03/31/government-internet-shutdowns-are-changing.-how-should-citizens-and-democracies-respond-pub-86687.

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

Freuler, Juan Ortiz. (2022). "Datafication & the Future of Human Rights Practice." JustLabs. https://www.openglobalrights.org/userfiles/file/Datafication_Report_JustLabs_2022.pdf.

Friedlaender, E., and F. Winston. (2004). "Evidence Based Advocacy." *Injury Prevention* 10, no. 6: 324–26. https://doi.org/10.1136/ip.2004.006536.

Garfinkel, Simson, and Heather Richter Lipford. (2014). "Usable Security: History, Themes, and Challenges." *Synthesis Lectures on Information Security, Privacy, and Trust* 5, no. 2: 1–124. https://doi.org/10.2200/S00594ED1V01Y201408SPT011.

Global Network Initiative. (2020). Increasing Transparency on Human Rights Due Diligence and Impact Assessments by GNI Company Members. Global Network Initiative. https://globalnetworkinitiative.org/increasing-transparency-on-human-rights-due-diligence-and-impact-assessments-by-gni-company-members/

Government of the United Kingdom. (2022). Press Release: World-first online safety laws introduced in Parliament. https://www.gov.uk/government/news/world-first-online-safety-laws-introduced-in-parliament

Green, Maria. (2001). What We Talk About When We Talk About Indicators: Current Approaches to Human Rights Measurement. Human Rights Quarterly 23. https://www.jstor.org/stable/4489371?seq=1.

Green, Natalie & Rossini, Carolina. (2015). Open Internet Course. Public Knowledge. https://publicknowledge.org/open-internet-course/

Hanson, Fergus. (2012). "Internet Freedom: The Role of the U.S. State Department." *Brookings*. https://www.brookings.edu/research/internet-freedom-the-role-of-the-u-s-state-department/.

Hanson, Fergus. (2012). "Baked in and Wired: EDiplomacy @ State." *Brookings*. https://www.brookings.edu/research/baked-in-and-wired-ediplomacy-state/.

Haristya, Sherly. (2020). "The Efficacy of Civil Society in Global Internet Governance." *Internet Histories* 4, no. 3: 252–70. https://doi.org/10.1080/24701475.2020.1769892.

Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi.

Henry, Ryan, Stacie L. Pettyjohn, and Erin York. (2014). "Portfolio Assessment of the Department of State Internet Freedom Program." RAND Corporation. https://www.rand.org/pubs/research_reports/RR794.html.

Holt, Jennifer, and Lisa Parks. (2021). "The Labor of Digital Privacy Advocacy in an Era of Big Tech." *Media Industries* 8, no. 1. https://doi.org/10.3998/mij.93.

———, "H.R.491 - 113th Congress (2013-2014): Global Online Freedom Act of 2013." *Congress.gov*, Library of Congress, 25 February 2013, http://www.congress.gov/.

———, "H.R.2075 - 117th Congress (2021-2022): Foreign Advanced Technology Surveillance Accountability Act." Congress.gov, March 19, 2021. http://www.congress.gov/.

Human Rights Watch. (2020). "Shutting Down the Internet to Shut Up Critics." https://www.hrw.org/world-report/2020/country-chapters/global-5.

Hynes, Casey. (2016). Digital Rights Must Become A Top Priority In Myanmar's Connectivity Revolution. Forbes. https://www.forbes.com/sites/chynes/2016/12/21/digital-rights-must-become-a-top-priority-in-myanmars-connectivity-revolution/?sh=659f29d02267.

Internet Policy Observatory. (2018). "Using Research in Digital Rights Advocacy: Understanding the Research Needs of the Internet Freedom Community." University of Pennsylvania. https://www.asc.upenn.edu/news-events/news/using-research-digital-rights-advocacy-understanding-research-needs-internet-freedom-community.

Internet Rights and Principles Coalition. (2014). The Charter of Human Rights and Principles for the Internet. Internet Governance Forum, United Nations. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf

Internet Society. (2016). Internet Governance – Why the Multistakeholder Approach Works. Internet Society. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

Ingram, George. (2020). "Civil Society: An Essential Ingredient of Development." *Brookings* (blog). https://www.brookings.edu/blog/up-front/2020/04/06/civil-society-an-essential-ingredient-of-development/.

Jassem, Manal Dawood, Amer Abdulmajeed Abdulrahman. (2022). Survey on Distributed Denial of Service Attack Detection Using Deep Learning: A Review. Int. J. Nonlinear Anal. Appl. In Press, 1 – 10. ISSN: 2008-6822. https://ijnaa.semnan.ac.ir/article_6458_8d4fe99cb1b53f375c13856578dbacf9.pdf

Kaare, Suma, Naved Chowdhury, and Vivian Kazi, eds. (2007). "The Power of Evidence in Advocacy: Resource Pack for Trainers on Evidence-Based Policy Advocacy in East Africa." *ODI: Think Change.* https://odi.org/en/publications/the-power-of-evidence-in-advocacy-resource-pack-for-trainers-on-evidence-based-policy-advocacy-in-east-africa/.

Komaitis, Konstantinos. (2021). Internet Safety Is the New Internet Freedom. Slate. https://slate.com/technology/2021/11/internet-safety-vs-internet-freedom.html

Krafchik, Warren. (2013). "Advocacy from the Inside: The Role of Civil Society." Stanford Social Innovation Review. https://ssir.org/articles/entry/advocacy_from_the_inside_the_role_of_civil_society.

Lamensch, Marie. (2021). For Rights Defenders, Cyber Is the New Battleground. Centre for International Governance Innovation. https://www.cigionline.org/articles/for-rights-defenders-cyber-is-the-new-battleground/

Leberknight, Christopher, et al. (2010). A Taxonomy of Internet Censorship (Draft Version). http://www.princeton.edu/~chiangm/anticensorship.pdf

Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23

Lutscher, Philipp M., Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti. (2019). "At Home and Abroad: The Use of Denial-of-Service Attacks during Elections in Nondemocratic Regimes." *Journal of Conflict Resolution* 64, no. 2-3: 373–401. https://doi.org/10.1177/0022002719861676.

MacKinnon, Rebecca. (2017). *Consent of the Networked: The Worldwide Struggle For Internet Freedom*. Basic Books.

Maréchal, Nathalie. (2015). Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate. International Journal of Communication 9. https://ijoc.org/index.php/ijoc/article/viewFile/3330/1494.

Media Defence. (2020). Encryption and Anonymity on the Internet. Media Defence, Advanced Modules on Digital Rights and Freedom of Expression Online. https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/encryption-and-anonymity-on-the-internet/

Murdie, Amanda. (2015). "The Importance of Evidence-Based Human Rights Advocacy." *The Duck of Minerva* (blog). https://www.duckofminerva.com/2015/11/the-importance-of-evidence-based-human-rights-advocacy.html.

Naqvi, Bilal, and Ahmed Seffah. (2018). "A Methodology for Aligning Usability and Security in Systems and Services." *3rd International Conference on Information Systems Engineering (ICISE)*, 61–66. https://doi.org/10.1109/ICISE.2018.00019.

Necessary & Proportionate. (2014). International Principles on the Application of Human Rights to Communications Surveillance. https://www.eff.org/files/necessaryandproportionatefinal.pdf

New America. (n.d.). Case Study #3: Transparency Reporting. New America, Getting Internet Companies To Do The Right Thing. https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/.

Newton, Casey. (2018). "Internet Freedom Continues to Decline around the World, a New Report Says." The Verge. https://www.theverge.com/2018/11/1/18050394/internet-freedom-report-2018-freedom-house-chertoff.

Newton-Small, Jay. (2012). "Hillary's Little Startup: How the U.S. Is Using Technology to Aid Syria's Rebels." *Time*. https://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/.

Nonprofit Association of Oregon. (2010). "Public Policy Advocacy: What, Why & How." https://nonprofitoregon.org/advocacy/nonprofit_advocacy.

Ochom, Jonathan. (2022). The Case For A Human Rights-Based Approach To Technology. Human Rights Pulse. https://www.humanrightspulse.com/mastercontentblog/the-case-for-a-human-rights-based-approach-to-technology

Oh, Sarah. (2017). Advocating for Openness: Nine Ways Civil Society Groups Have Mobilized to Defend Internet Freedom. CIMA. https://www.cima.ned.org/publication/advocating-openness-nine-ways-civil-society-groups-mobilized-defend-internet-freedom/

OHCHR. (2014). "OHCHR | Civil Society Space and the United Nations Human Rights System - A Practical Guide for Civil Society." https://www.ohchr.org/en/publications/civil-society-space-and-united-nations-human-rights-system-practical-guide-civil.

Open Internet for Democracy. (2021). "Open Internet for Democracy Advocacy Playbook." https://openinternet.global/resources/open-internet-playbook.

Open Technology Fund. (n.d.). Rapid Response Fund. https://www.opentech.fund/funds/rapid-response-fund/

Penney, Jonathan and Sarah McKune, Lex Gill, Ronald J. Deibert. (2018). Advancing Human Rights By Design In The Dual-Use Technology Industry. Columbia Journal of International Affairs. https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry

Purcell, Fuatai, Guyverson Vernous, Shahid Akbar, and Susana Finquelievich. (2006). Review of *Role of Civil Society: Internet Governance and Developing Countries*, by Veronica Cretu and Valentin Katrandjiev. Internet Governance Research Project, DiploFoundation. http://archive1.diplomacy.edu/pool/fileInline.php?IDPool=129.

Remensperger, John & Schwartz-Henderson, Laura & Cendic, Kristina. (2018). Using Research in Digital Rights Advocacy: Understanding the Research Needs of the Internet Freedom Community. Internet Policy Observatory. https://www.asc.upenn.edu/sites/default/files/2021-02/using-research-in-digital-rights-advocacy-internet-policy-observatory.pdf

Repucci, Sarah and Slipowitz, Amy. (2022). The Global Expansion of Authoritarian Rule. Freedom House. https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva. (2015). "Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals." RAND Corporation. https://www.rand.org/pubs/research_reports/RR1151.html.

Ryan-Mosley, Tate. (2021). Why you should be more concerned about internet shutdowns. MIT Technology Review. https://www.technologyreview.com/2021/09/09/1035237/internet-shutdowns-censorship-exponential-jigsaw-google/?utm_source=pocket_mylist

Shabaz, Adrian and Funk, Allie. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

Shabaz, Adrian and Funk, Allie. (2020). Freedom on the Net 2020: The Pandemic's Digital Shadow. Freedom House. https://freedomhouse.org/report/report-sub-page/2020/policy-recommendations-freedom-net-2020#:~:text=Studies%20and%20surveys%20have%20shown,back%20against%20shutdowns%20and%20censorship.

Schneier, Bruce. (2018). Human Rights by Design. Schneier on Security. https://www.schneier.com/blog/archives/2018/12/human_rights_by.html

Smith, Christopher H. (n.d.). Global Online Freedom Act of 2013, Pub. L. No. H.R.491.

Sovran, Yair, Jinyang Li, and Lakshminarayanan Subramanian. (n.d.). "Unblocking the Internet: Social Networks Foil Censors." Computer Science Department, New York University.

Stjernfelt, Frederik, and Anne Mette Lauritzen. (2020). "The Role of Civil Society." In *Your Post Has Been Removed: Tech Giants and Freedom of Speech*. Springer International Publishing. https://doi.org/10.1007/978-3-030-25968-6_17.

The Global Handwashing Partnership. (2017). Event Summary: From Research to Advocacy–Using evidence to drive change. https://globalhandwashing.org/from-research-to-advocacy-using-evidence-to-drive-change-summary/.

Trionfi, Barbara, and Javier Luque. (2019). "Newsroom Best Practices for Addressing Online Violence against Journalists." IPI. https://newsrooms-ontheline.ipi.media/newsroom-best-practices-for-addressing-online-violence-against-journalists/.

Tsampi, Aikaterini. (2021). The Role of Civil Society in Monitoring the Executive in the Case-Law of the European Court of Human Rights: Recasting the Rule of Law. Utrecht Law Review, 17(2). http://doi.org/10.36633/ulr.671

United States Government. (n.d.). "Strengthen and Protect Civil Society, Recognizing the Essential Role of Local Capacity in Advancing Democratic Governance and Human Rights | Performance.Gov." https://obamaadministration.archives.performance.gov/content/strengthen-and-protect-civil-society-recognizing-essential-role-local-capacity-advancing.html.

United Nations Department of Peacekeeping Operations and UN Department for Field Support. (2017). "Understanding and Improving Engagement with Civil Society in UN Peacekeeping: From Policy to Practice." http://dag.un.org/handle/11176/400649.

United Nations General Assembly, Human Rights Council. (2016). Oral Revisions of 30 June. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

United Nations General Assembly. (1966). International Covenant on Civil and Political Rights, Art. 19. United Nations General Assembly Resolution 2200A. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

USAID. Privacy Basics. (2014). United States Government. https://www.usaid.gov/sites/default/files/documents/1868/508saa.pdf

USAID. (2021). "Supporting Vibrant Civil Society & Independent Media | Democracy, Human Rights and Governance | U.S. Agency for International Development." https://www.usaid.gov/democracy/supporting-vibrant-civil-society-independent-media.

U.S. Department of State. (n.d.) "Briefing on Internet Freedom and 21st Century Statecraft." //2009-2017.state.gov/j/drl/rls/rm/2010/134306.htm.

US Department of State, Bureau of Democracy, Human Rights, and Labor. (2021) DRL FY22 Internet Freedom Annual Program Statement. US Department of State.

U.S. Mission to the United Nations in Geneva. (2006). "Secretary of State Establishes New Global Internet Freedom Task Force," press release. http://geneva.usmission.gov/Press2006/02141InternetTaskForce.html

Vioreanu, Dana. (2021). "Privacy by Design Principles: Why Data Protection Should Always Come First," CyberGhost Privacy Hub. https://www.cyberghostvpn.com/privacyhub/privacy-by-design-principles-why-data-protection-should-always-come-first/.

Watershed. (2020). "Evidence-Based Advocacy: How Civil Society Generates and Uses Evidence for Influencing Policy." https://watershed.nl/media/evidence-based-advocacy-how-civil-society-generates-and-uses-evidence-for-influencing-policy-and-practice/.

Weinberg, Friedhelm. (2019). 3 ways activists are being targeted by cyberattacks. World Economic Forum. https://www.weforum.org/agenda/2019/05/3-ways-activists-targeted-online-cybersecurity/

West, Ben. (2021). Crime and Technology, Part 1: Secure Communication Platforms. Stratfor. https://worldview.stratfor.com/article/crime-and-technology-part-i-secure-communication-platforms?utm_source=pocket_mylist

World Economic Forum. (2022). The Global Risks Report 2022. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Young, E. & Quinn, L. (2012). Making Research Evidence Matter: A guide to policy advocacy in transition countries. International Centre for Policy Advocacy. https://advocacyguide.icpolicyadvocacy.org/236-what-is-the-goal-of-policy-advocacy#fn:236

Zuckerman, E. et al. (2010). Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites. The Berkman Center for Internet & Society at Harvard University.

https://www.opensocietyfoundations.org/uploads/88c8cc50-b839-4250-a2ea-f045940565b8/Political-DDoS-20110106.pdf

ANNEX 5. PILLAR GOALS, VALUES, LINES OF EFFORT AND THEORIES OF CHANGE

Pillar 1. Technology Development

GOAL

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.

- Unrestricted access to the global internet in censored environments
- Surveillance-free communications for users
- Websites are protected from the most common forms of DDoS attacks
- Freedom of Expression is maintained

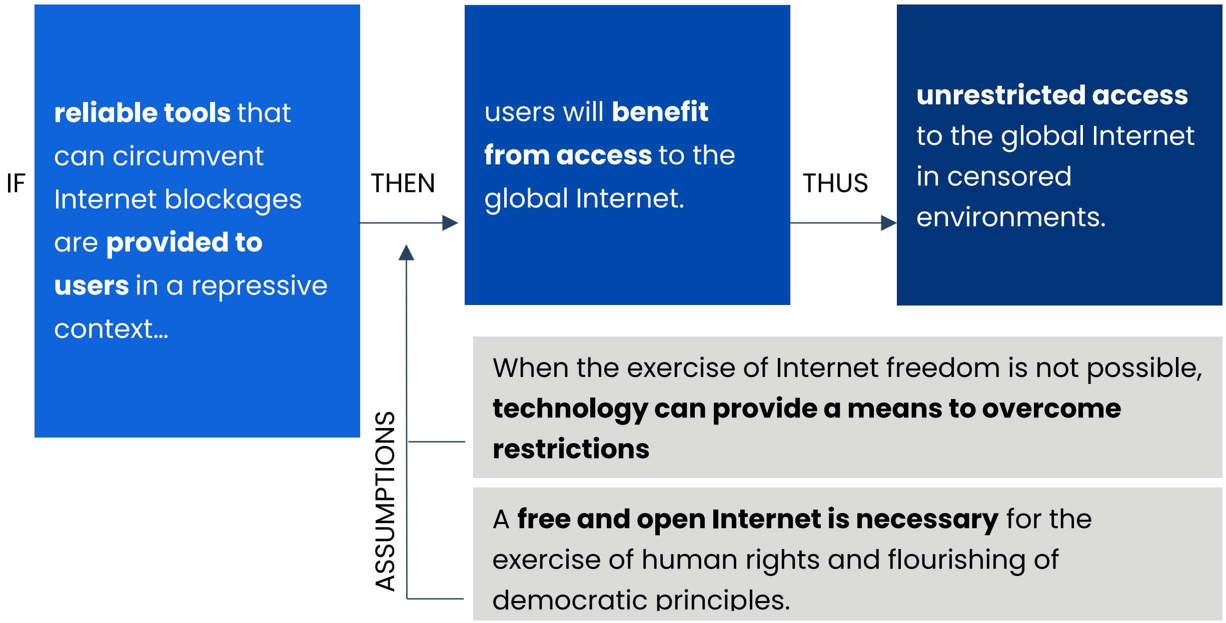
VALUES

- Freedom of Expression, Freedom to Access Information, and Privacy are fundamental, and apply equally online.
- Support open source and interoperable technology.
- Operational methodologies are generally transparent.
- Independent third-party security auditing for all user-facing tech consistent with industry standards.
- Transparent usage data.
- User-centered design ("build with, not for") and usability.
- Privacy for users (with a strong preference for "privacy by design").
- Technology must serve Human Rights goals.
- Technology is generally "content agnostic."
- Target the security needs of vulnerable populations online

LINES OF EFFORT

1. Anti-Censorship Tech
2. Secure Communications
3. Peer-to-Peer Communications
4. DDoS Mitigation
5. Small Grants

Figure 4. Anti-Censorship Theory of Change



IF **reliable tools** that can circumvent Internet blockages are **provided to users** in a repressive context…

THEN users will **benefit from access** to the global Internet.

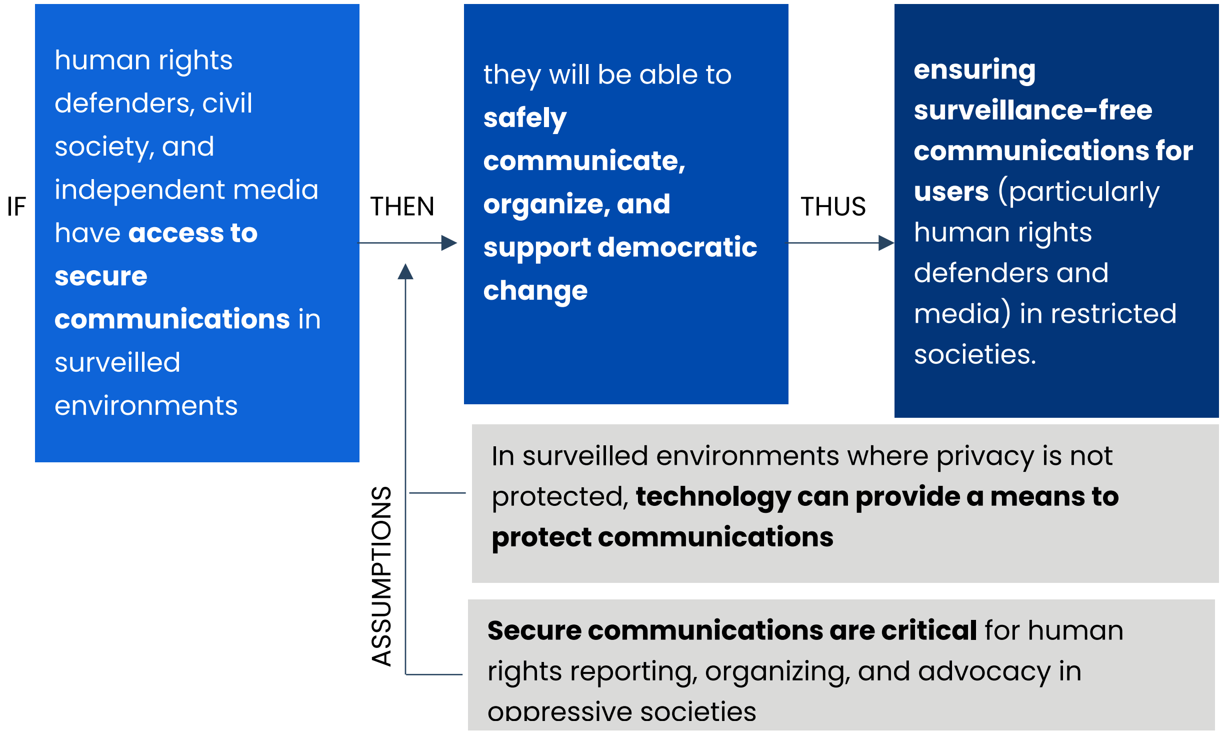
THUS **unrestricted access** to the global Internet in censored environments.

ASSUMPTIONS

When the exercise of Internet freedom is not possible, **technology can provide a means to overcome restrictions**

A **free and open Internet is necessary** for the exercise of human rights and flourishing of democratic principles.

Figure 5. Secure Communication Theory of Change



IF human rights defenders, civil society, and independent media have **access to secure communications** in surveilled environments

THEN they will be able to **safely communicate, organize, and support democratic change**

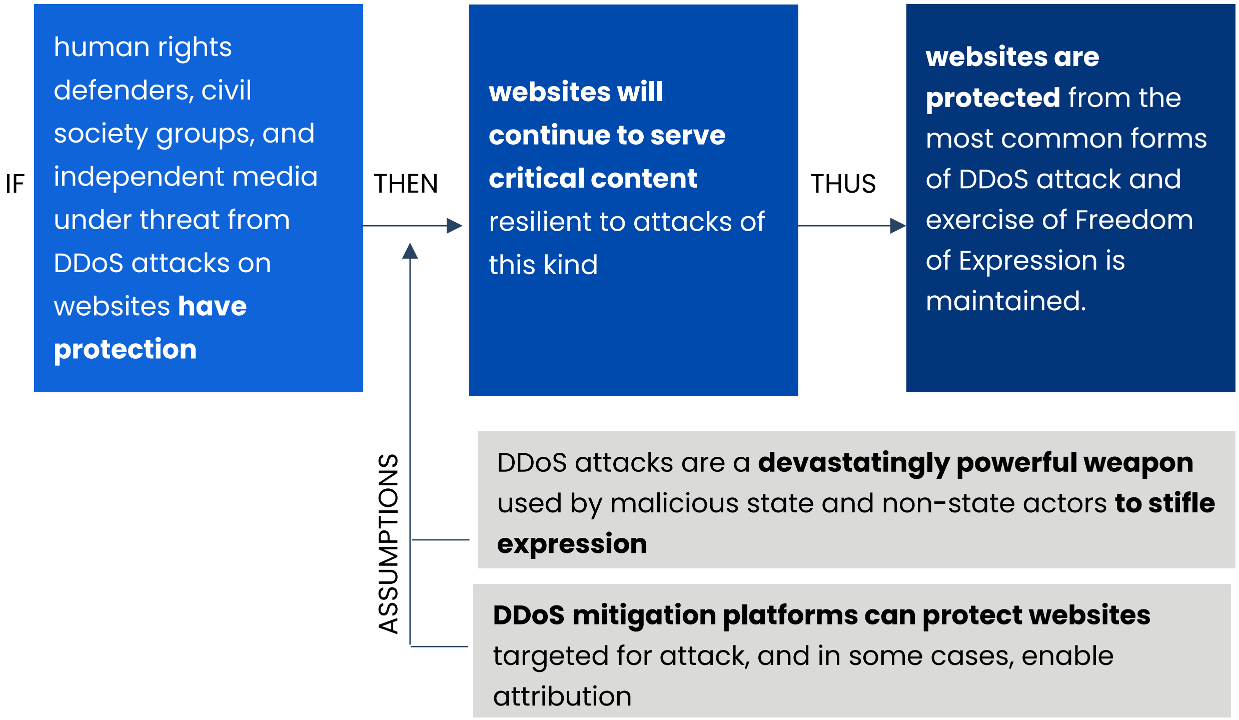
THUS **ensuring surveillance-free communications for users** (particularly human rights defenders and media) in restricted societies.

ASSUMPTIONS

In surveilled environments where privacy is not protected, **technology can provide a means to protect communications**

Secure communications are critical for human rights reporting, organizing, and advocacy in oppressive societies

Figure 6. DDoS Mitigation Theory of Change



IF

human rights defenders, civil society groups, and independent media under threat from DDoS attacks on websites **have protection**

THEN

websites will continue to serve critical content resilient to attacks of this kind

THUS

websites are protected from the most common forms of DDoS attack and exercise of Freedom of Expression is maintained.

ASSUMPTIONS

DDoS attacks are a **devastatingly powerful weapon** used by malicious state and non-state actors **to stifle expression**

DDoS mitigation platforms can protect websites targeted for attack, and in some cases, enable attribution

Pillar 2. Digital Safety

GOAL

Enhance digital security training and capacity building for democracy activists to combat violence against bloggers and other users.

- Civil society is able to work effectively under adverse circumstance
- Civil society is prepared and resilient in the face of digital threats
- Damage of digital attacks on civil society is mitigated
- CSOs can resume and continue work effectively
- Civil society is able to exercise fundamental rights and freedoms online
- Civil society better understands digital security risks
- Civil society can prevent and respond to digital security threats
- Civil society knows where they can get digital security support
- Education and awareness raising for vulnerable populations directly responds to their needs

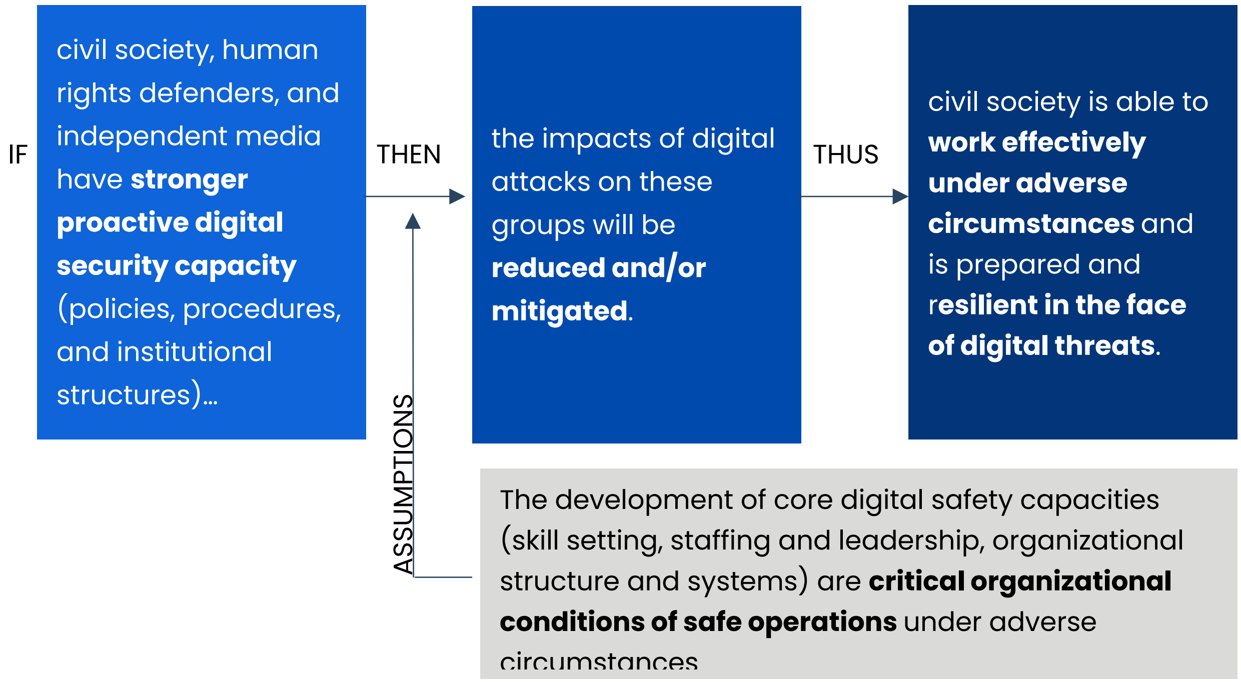
VALUES

- Promote holistic security (digital, physical, and psychosocial)
- Digital literacy is a building block of security education
- Practice do no harm & harm reduction
- Human- and privacy-oriented security training (vs. cybersecurity)
- A time-sensitive response to attacks is critical
- Culture of safety vs. culture of risk-taking: changing the culture of huma rights and media work
- Promote risk assessment & management theory and practice
- When dealing with organizations, obtain buy-in from the highest level
- Target the security needs of vulnerable populations online

LINES OF EFFORT

6. Digital Security Capacity-Building
7. Emergency Support
8. Public Awareness-Raising & Education

Figure 7. Digital Safety Capacity Building Theory of Change



IF

civil society, human rights defenders, and independent media have **stronger proactive digital security capacity** (policies, procedures, and institutional structures)…

THEN

the impacts of digital attacks on these groups will be **reduced and/or mitigated**.

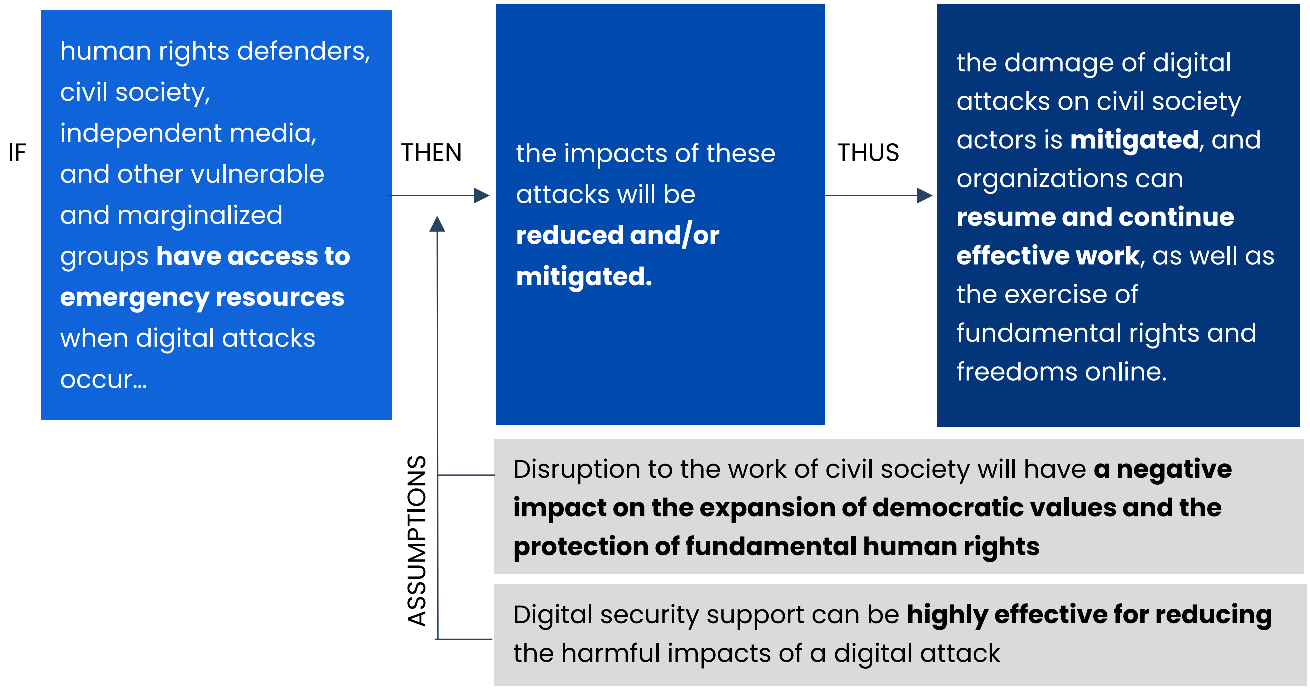
THUS

civil society is able to **work effectively under adverse circumstances** and is prepared and **resilient in the face of digital threats**.

ASSUMPTIONS

The development of core digital safety capacities (skill setting, staffing and leadership, organizational structure and systems) are **critical organizational conditions of safe operations** under adverse circumstances

Figure 8. Emergency Support Theory of Change



IF

human rights defenders, civil society, independent media, and other vulnerable and marginalized groups **have access to emergency resources** when digital attacks occur…

THEN

the impacts of these attacks will be **reduced and/or mitigated.**

THUS

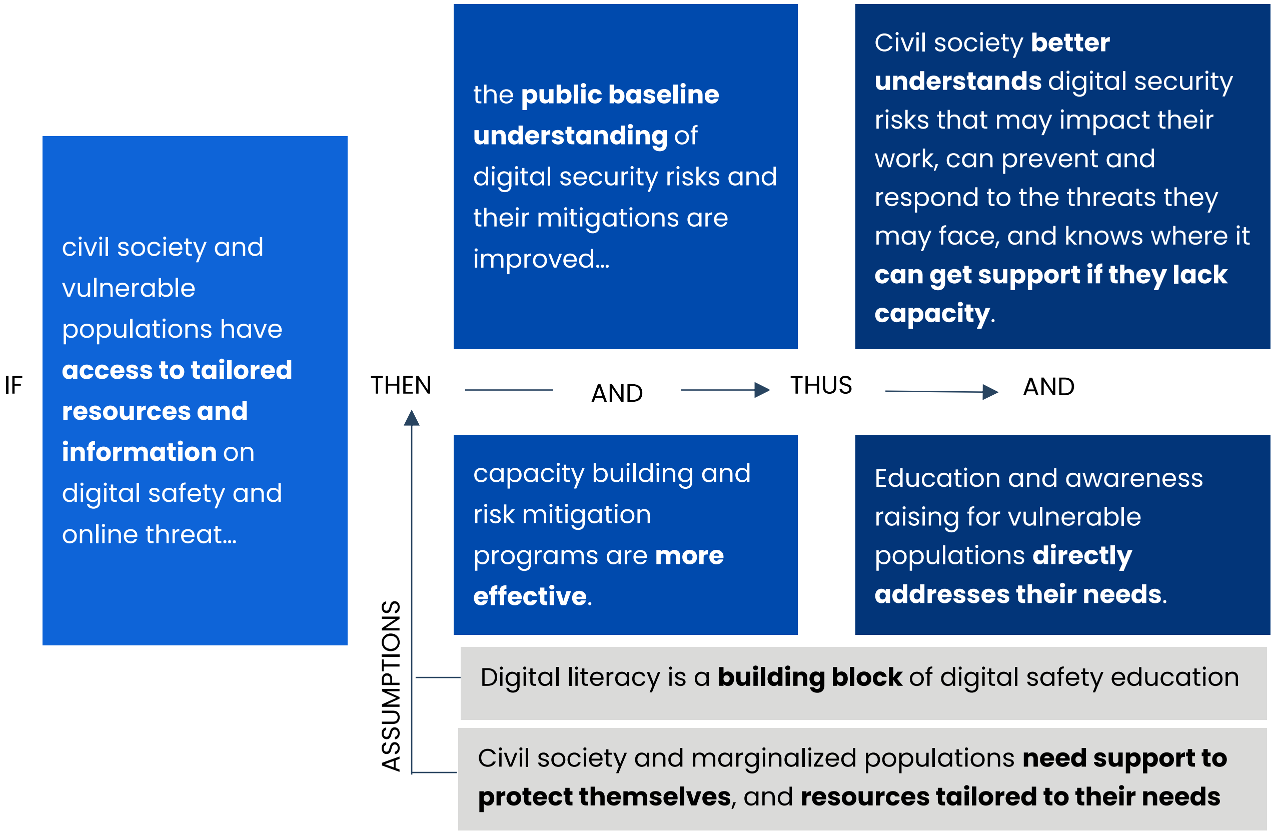
the damage of digital attacks on civil society actors is **mitigated**, and organizations can **resume and continue effective work**, as well as the exercise of fundamental rights and freedoms online.

ASSUMPTIONS

Disruption to the work of civil society will have **a negative impact on the expansion of democratic values and the protection of fundamental human rights**

Digital security support can be **highly effective for reducing** the harmful impacts of a digital attack

Figure 9. Public Awareness Raising and Education Theory of Change



IF

civil society and vulnerable populations have **access to tailored resources and information** on digital safety and online threat…

THEN

the **public baseline understanding** of digital security risks and their mitigations are improved…

AND

capacity building and risk mitigation programs are **more effective**.

THUS

Civil society **better understands** digital security risks that may impact their work, can prevent and respond to the threats they may face, and knows where it **can get support if they lack capacity**.

AND

Education and awareness raising for vulnerable populations **directly addresses their needs**.

ASSUMPTIONS

Digital literacy is a **building block** of digital safety education

Civil society and marginalized populations **need support to protect themselves**, and **resources tailored to their needs**

Pillar 3. Legal Advocacy

GOAL

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.

- CSOs successfully advocate for the protection of human rights online
- Civil society has access and capacity to advocate for human rights in multi-stakeholder technology policy and standards-setting fora.
- Institutions respect the place of Internet freedom as a central human rights issue.
- CSOs have the capacity and expertise to advocate for Internet freedom as a central human rights issue.
- ICT companies adopt and abide by policies and practices that respect and protect human rights
- Legal advocacy protects at-risk and marginalized individuals from repressive laws that restrict freedom of expression

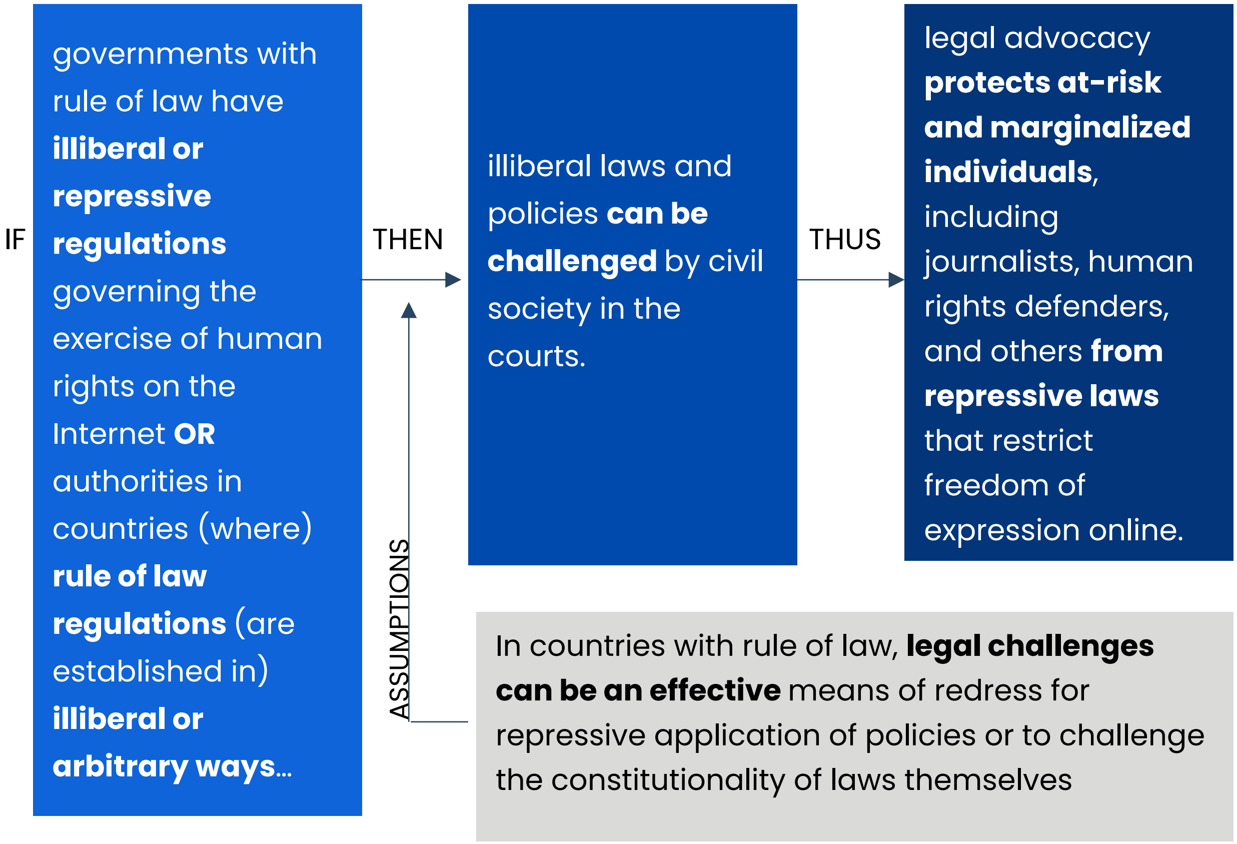
VALUES

- Human rights on the global Internet are a critical set of adjacent and legitimate rights
- Empower local organizations to advocate locally
- Go beyond capacity-building, strategize for concrete change
- Engage with businesses, and promote the Voluntary Principles and HRIAs
- Normalize international human rights standards in tech policy
- Bring tech policy into traditionally non-tech HR advocacy spaces
- Advocate locally, regionally, and globally. Understand processes at all levels
- Advocacy is informed by deep technical understanding

LINES OF EFFORT

9. Human Rights in Internet Policy
10. Internet Freedom in Human Rights Policy
11. Internet Freedom/ Business & Human Rights
12. Legal Advocacy

Figure 10. Legal Advocacy Theory of Change



IF

governments with rule of law have **illiberal or repressive regulations** governing the exercise of human rights on the Internet **OR** authorities in countries (where) **rule of law regulations** (are established in) **illiberal or arbitrary ways…**

THEN

illiberal laws and policies **can be challenged** by civil society in the courts.

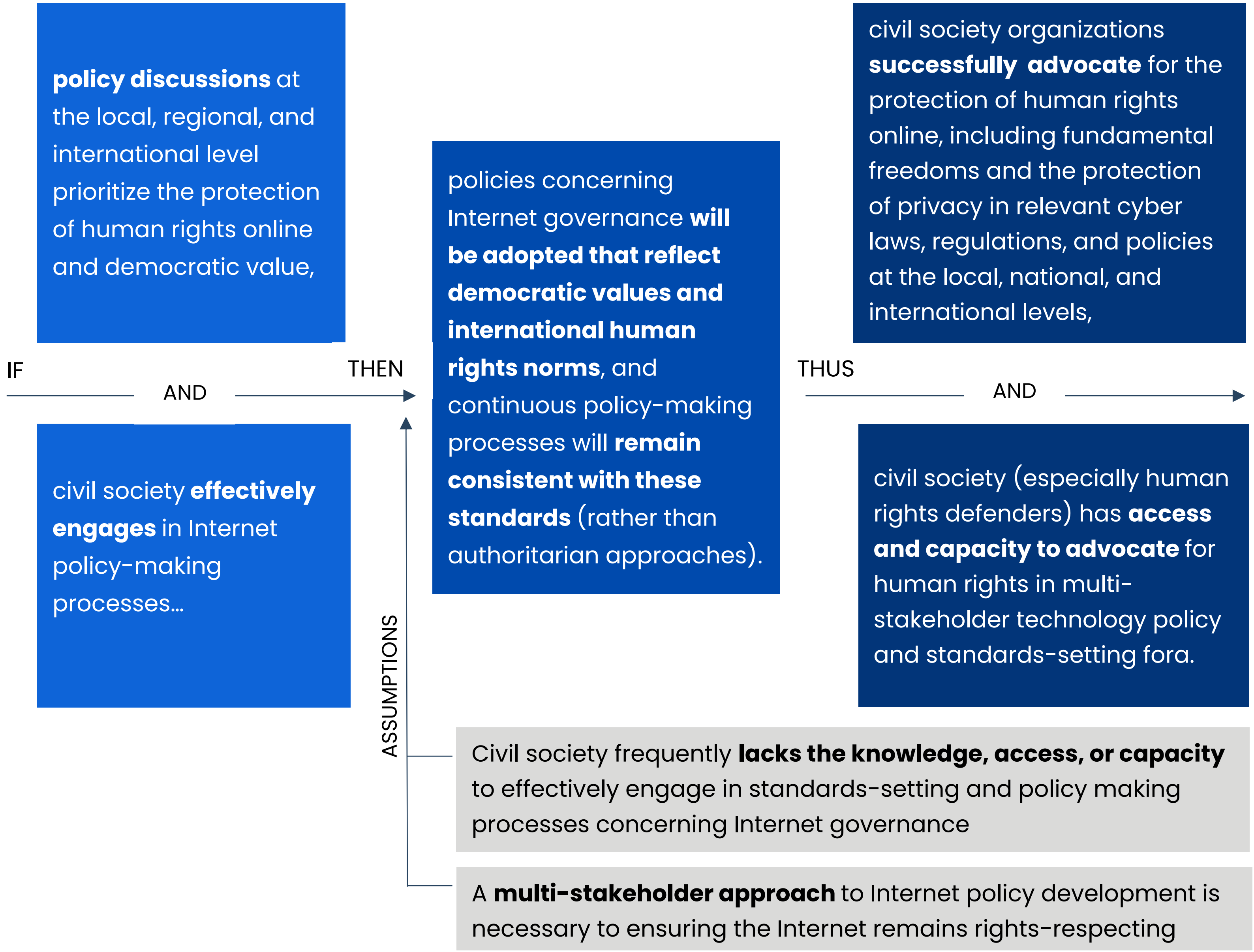
THUS

legal advocacy **protects at-risk and marginalized individuals,** including journalists, human rights defenders, and others **from repressive laws** that restrict freedom of expression online.

ASSUMPTIONS

In countries with rule of law, **legal challenges can be an effective** means of redress for repressive application of policies or to challenge the constitutionality of laws themselves

Figure 11. Human Rights in Internet Policy Theory of Change



IF

policy discussions at the local, regional, and international level prioritize the protection of human rights online and democratic value,

AND

civil society **effectively engages** in Internet policy-making processes...

THEN

policies concerning Internet governance **will be adopted that reflect democratic values and international human rights norms**, and continuous policy-making processes will **remain consistent with these standards** (rather than authoritarian approaches).

THUS

civil society organizations **successfully advocate** for the protection of human rights online, including fundamental freedoms and the protection of privacy in relevant cyber laws, regulations, and policies at the local, national, and international levels,

AND

civil society (especially human rights defenders) has **access and capacity to advocate** for human rights in multi-stakeholder technology policy and standards-setting fora.

ASSUMPTIONS

Civil society frequently **lacks the knowledge, access, or capacity** to effectively engage in standards-setting and policy making processes concerning Internet governance

A **multi-stakeholder approach** to Internet policy development is necessary to ensuring the Internet remains rights-respecting

Pillar 4. Research

GOAL

Research key threats to Internet freedom

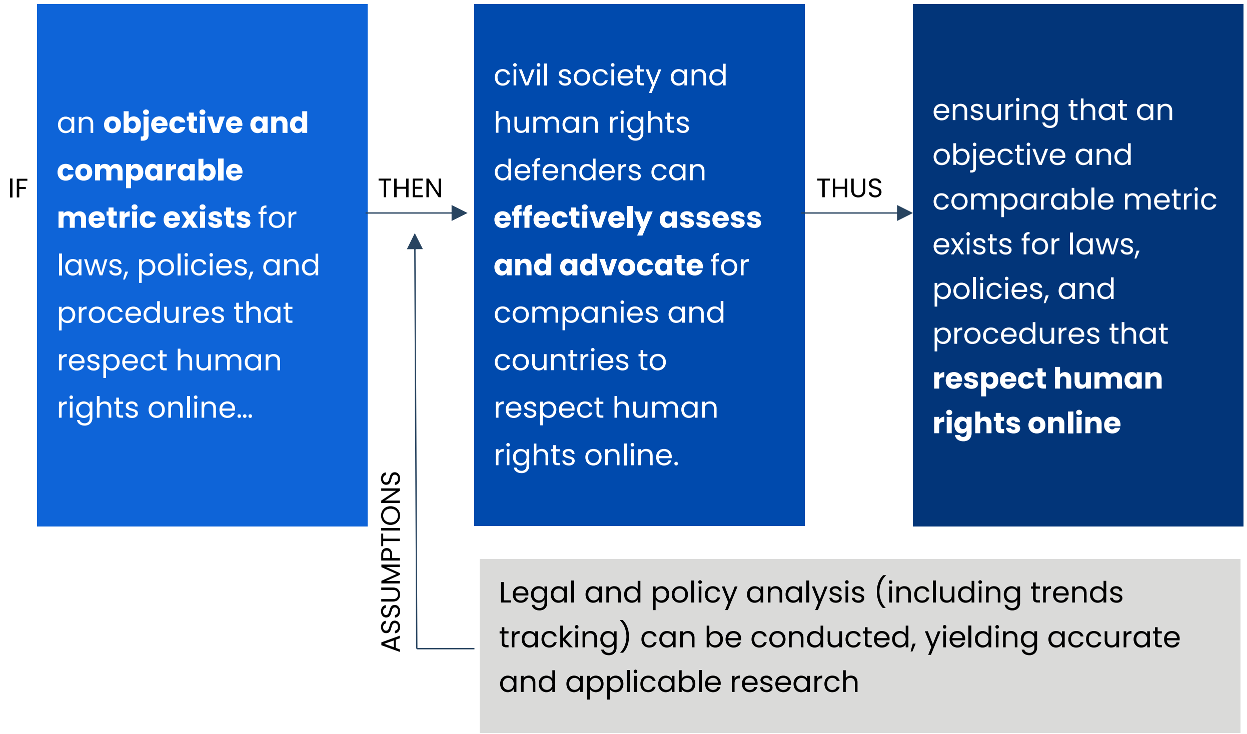
VALUES

- Research drives everything. Optimize data for use by advocates, security trainers, and technologists
- Research outputs are open-source and for the public good
- Encourage the sharing of threat intelligence
- Collaborate effectively. No competitive data hoarding, or undercutting other efforts
- Protect user privacy and safety. Conform to data ethics and informed consent standards

LINES OF EFFORT

13. Global Rankings
14. Censorship Measurement

Figure 12. Global Rankings Theory of Change



an **objective and comparable metric exists** for laws, policies, and procedures that respect human rights online...

civil society and human rights defenders can **effectively assess and advocate** for companies and countries to respect human rights online.

ensuring that an objective and comparable metric exists for laws, policies, and procedures that **respect human rights online**

Legal and policy analysis (including trends tracking) can be conducted, yielding accurate and applicable research

ANNEX 6. ENDNOTES

[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/

[3] KII 16

[4] KII 9

[5] "Internet Freedom Theory of Change and Strategic Framework": Internet Freedom Program, State/DRL, undated.

[6] "Functional Bureau Strategies": DRL, 2015–2021.

[7] National Cyber Strategy of the United States of America: The Office of the President, 2018.

[8] Consolidated Appropriations Acts: 2015–2021.

[9] DRL/GP FY22 Internet Freedom Annual Program Statement.

[10] DRL/GP FY22 Internet Freedom Annual Program Statement.

[11] "Internet Freedom, Theory of Change, and Strategic Framework": DRL/GP PowerPoint presentation, undated.

[12] Internet Freedom, Strategic Framework

[13] U.S. Department of State Bureau of Democracy, Human Rights, and Labor. (2022). Functional Bureau Strategy. https://www.state.gov/wp-content/uploads/2022/08/FBS_DRL_Public.pdf

[14] https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[15] Doc21

[16] KII 15

[17] https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

[18] KII 16

[19] KII 9

[20] Consolidated Appropriations Act 2020, Section 705

[21] DOC 21

[22] Doc 22

[23] IF Indicator Reference Sheet https://devtechsys.sharepoint.com/:b:/s/DOS-InternetFreedom/EVpBklEbzgBAnelSpAVipJ8BsS99-uDyOVTFKjWUtqnJqQ?e=yeYWnL

[24] FGD 4

[25] Doc 13

[26] Doc 14

[27] FGD 2

[28] FGD 2

[29] FGD 2

[30] FGD 2

[31] FGD 2

[32] Doc 21 and FGD 13

[33] Doc 22

[34] FGD 7

[35] IF Indicator Reference Sheet https://devtechsys.sharepoint.com/:b:/s/DOS-InternetFreedom/EVpBklEbzgBAnelSpAVipJ8BsS99-uDyOVTFKjWUtqnJqQ?e=yeYWnL

[36] FGD 7

[37] FGD 2

[38] FGD 13

[39] FGD 7

[40] FGD 2

[41] FGD 13

[42] FGD 7

[43] FGD 2

[44] FGD 13

[45] Repucci, Sarah and Slipowitz, Amy. (2022). The Global Expansion of Authoritarian Rule. Freedom House. https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf
[46] FGD 4
[47] KII 7
[48] KII 4
[49] KII 4
[50] KII 2
[51] KII 4
[52] Human Rights Watch. "Shutting Down the Internet to Shut Up Critics." In English, 2020. https://www.hrw.org/world-report/2020/country-chapters/global-5
[53] Cui, Jingbo. (2021). Network Censorship. McKelvey School of Engineering, Computer Science & Engineering. https://www.cse.wustl.edu/~jain/cse570-21/ftp/pearg.pdf
[54] KII 8
[55] KII 8
[56] KII 10
[57] KII 2
[58] KII 2
[59] KII 4
[60] Ammarah Cheema, Moeenuddin Tariq, Adnan Hafiz, Muhammad Murad Khan, Fahad Ahmad, Muhammad Anwar, "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review", Security and Communication Networks, vol. 2022, Article ID 8379532, 15 pages, 2022. https://doi.org/10.1155/2022/8379532
[61] Ammarah Cheema, Moeenuddin Tariq, Adnan Hafiz, Muhammad Murad Khan, Fahad Ahmad, Muhammad Anwar, "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review", Security and Communication Networks, vol. 2022, Article ID 8379532, 15 pages, 2022. https://doi.org/10.1155/2022/8379532
[62] CISA, Understanding Denial-of-Service Attacks, November 2019. https://www.uscert.gov/ncas/tips/ST04-015
[63] European Union Agency for Cybersecurity (ENISA), (2021), "ENISA Threat Landscape 2021." https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[64] FGD 7
[65] Pandemic DDoS Attack Activity NETSCOUT Threat Intelligence Report
[66] KII 10
[67] KII 4
[68] KII 13
[69] KII 10
[70] KII 9
[71] KII 9
[72] KII 8
[73] KII 13
[74] KII 7
[75] KII 9
[76] KII 9
[77] KII 4
[78] KII 2
[79] KII 4
[80] US Department of State, Bureau of Democracy, Human Rights, and Labor. (2021) DRL FY22 Internet Freedom Annual Program Statement. US Department of State.
[81] United States Congress. (2020). Consolidated Appropriations Act, Section 705. United States Government
[82] Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva. (2015). "Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals." RAND Corporation. https://www.rand.org/pubs/research_reports/RR1151.html.

[83] Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva. (2015). "Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals." RAND Corporation. https://www.rand.org/pubs/research_reports/RR1151.html.

[84] 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

[85] https://www.eff.org/issues/privacy

[86] Electronic Frontier Foundation. (n.d.). Anonymity. Electronic Frontier Foundation. https://www.eff.org/issues/anonymity

[87] Electronic Frontier Foundation. (n.d.). Anonymity. Electronic Frontier Foundation. https://www.eff.org/issues/anonymity

[88] Association for Progressive Communications. (2015). The right to freedom of expression and the use of encryption and anonymity in digital communications. Association for Progressive Communications. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/AssociationForProgressiveCommunication.pdf

[89] The evaluation team understands "illicit use" or "illicit purposes" to be synonymous with criminal activity as defined by the U.S. or international law and/or that "reflect any type of support for any member, affiliate, or representative of a designated terrorist organization". (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/)

[90] S.3764 – Internet Freedom and Operations (INFO) Act of 2022. 117th Congress (2021-2022)

[91] DRL/GP. Summary of DRL Internet Freedom Use Mitigation Strategy

[92] DRL/GP. Summary of DRL Internet Freedom Use Mitigation Strategy

[93] Penney, Jonathan and Sarah McKune, Lex Gill, Ronald J. Deibert. (2018). Advancing Human-Rights-By-Design In The Dual-Use Technology Industry. Columbia Journal of International Affairs. https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry

[94] Penney, Jonathon, Sarah Mckune, Lex Gill, and Ronald J. Deibert. (2018). Advancing Human-Rights-by-Design in the Dual-Use Technology Industry. Journal of International Affairs. Colombia School of International and Public Affairs. https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry

[95] DRL/GP. Summary of DRL Internet Freedom Use Mitigation Strategy

[96] KII 3

[97] West, Ben. (2021). Crime and Technology, Part 1: Secure Communication Platforms. Stratfor. https://worldview.stratfor.com/article/crime-and-technology-part-i-secure-communication-platforms?utm_source=pocket_mylist

[98] DRL defines "marginalized populations" as "people who are suffering under repression of human rights" (Interview with DRL) and "women, people with disabilities, racial and ethnic minorities, religious minorities, and lesbian, gay, bisexual and transgender (LGBT) people" (Full Proposal GOR Analysis Template).

[99] KII 3

[100] Penney, Jonathan and Sarah McKune, Lex Gill, Ronald J. Deibert. (2018). Advancing Human-Rights-By-Design In The Dual-Use Technology Industry. Columbia Journal of International Affairs.

[101] Romanosky, Sasha, Martin C. Libicki, Zev Winkelman, and Olesya Tkacheva. (2015). "Internet Freedom Software and Illicit Activity: Supporting Human Rights Without Enabling Criminals." RAND Corporation. https://www.rand.org/pubs/research_reports/RR1151.html.

[102] Expert Panel

[103] DRL/GP Representative

[104] FGD 18

[105] FGD 18

[106] https://www.ohchr.org/en/press-releases/2022/03/data-protection-systems-must-find-balance-between-protecting-privacy-and

[107] Follow-Up Interview 1

[108] Follow-Up Interview 2

[109] FGD 2

[110] FGD 2

[111] Expert Panel

[112] FGD 4
[113] Technology Project C. Final Project Narrative.
[114] Technology Project C. Final Project Narrative.
[115] Expert Panel
[116] Technology Project D. Updated Scope of Work
[117] Expert Panel
[118] FGD 4
[119] West, Ben. (2021). Crime and Technology, Part 1: Secure Communication Platforms. Stratfor. https://worldview.stratfor.com/article/crime-and-technology-part-i-secure-communication-platforms?utm_source=pocket_mylist
[120] FGD 13
[121] Focus Group Discussion with Grantee
[122] Technology Project B. Project Narrative.
[123] FGD 4
[124] Internal Risk Assessment Template and GOR Monitoring
[125] FGD 18
[126] DRL Internet Freedom Use Mitigation Strategy.
[127] Consolidated Appropriations Act 2020, Section 705
[128] Doc 39
[129] Doc 34
[130] Doc 39
[131] FGD 10
[132] FGD 12 and FGD 18
[133] FGD 12
[134] FGD 12
[135] FGD 16
[136] Doc 32 and FGD 15
[137] Doc 50
[138] Doc 50
[139] FGD 3
[140] Doc 56
[141] Doc 56 and FGD 3
[142] Doc 32 and Doc 34
[143] Doc 32
[144] FGD 15
[145] Doc 32
[146] KII 16
[147] Doc 38
[148] Doc 29
[149] Doc 38
[150] FGD 12
[151] FGD 10
[152] Doc 56
[153] Doc 63
[154] FGD 9
155 Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi
156 Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi
[157] FGD3
[158] FGD3

[159] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23
[160] FGD 15
[161] KII 9
[162] Levy, J., & Gillum, K. (2018). Tackling Digital Security Across Civil Society. Stanford Social Innovation Review. https://doi.org/10.48558/VVTN-6X23
[163] Shabaz, Adrian and Funk, Allie. (2020). Freedom on the Net 2020: The Pandemic's Digital Shadow. Freedom House. https://freedomhouse.org/report/report-sub-page/2020/policy-recommendations-freedom-net-2020#:~:text=Studies%20and%20surveys%20have%20shown,back%20against%20shutdowns%20and%20censorship.
[164] Henrichsen, Jennifer R., Michelle Betz, and Joanne Lisosky. (2015). "Building Digital Safety for Journalism: A Survey of Selected Issues." UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000232358/PDF/232358eng.pdf.multi.
[165] Shabaz, Adrian and Funk, Allie. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf
[166] Open Internet for Democracy. (2021). "Open Internet for Democracy Advocacy Playbook." https://openinternet.global/resources/open-internet-playbook.
[167] Collett, Robert, Nayia Barmpaliou, Patryk Pawla. (2021). International Cyber Capacity Building: Global Trends and Scenarios. European Commission. https://www.iss.europa.eu/content/international-cyber-capacity-building-global-trends-and-scenarios
[168] KII 15
[169] KII 5
[170] KII 4
[171] KII 4
[172] FGD 3
[173] FGD 16
[174] KII 14
[175] KII 14
[176] Consolidated Appropriations Act 2020, Section 705
[177] Doc 71, Doc 75, Doc 79
[178] Doc 75
[179] Doc 71
[180] Doc 75
[181] Doc 73
[182] Doc 71
[183] FGD 17
[184] FGD 1
[185] Doc 71
[186] Doc 83
[187] FGD 1
[188] FGD 1
[189] FGD 1
[190] FGD 17
[191] FGD 17
[192] FGD 14
[193] FGD 14
[194] FGD 14
[195] FGD 1
[196] FGD 1
[197] KII 16
[198] FGD 1
[199] FGD 17
[200] United Nations. (n.d.). Human Rights. https://www.un.org/en/global-issues/human-rights

[201] Shahbaz, A. & Funk, A. (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf
[202] KII 4
[203] KII 10
[204] KII 10
[205] KII 17
[206] KII 16
[207] KII 10
[208] KII 16
[209] KII 16
[210] KII 6
[211] Internet Society. (2016). Internet Governance – Why the Multistakeholder Approach Works. Internet Society. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/
[212] KII 10
[213] KII 10
[214] KII 4
[215] KII 4
[216] KII 4
[217] KII 2
[218] Consolidated Appropriations Act 2020, Section 705
[219] Doc 92
[220] Doc 98
[221] FGD 8
[222] FGD 8
[223] Doc 92
[224] Doc 98
[225] Doc 92
[226] Doc 92
[227] FGD 8
[228] FGD 6
[229] FGD 6
[230] FGD 6
[231] FGD 6
[232] Green, Maria. (2001). What We Talk About When We Talk About Indicators: Current Approaches to Human Rights Measurement. Human Rights Quarterly 23. https://www.jstor.org/stable/4489371?seq=1
[233] Green, Maria. (2001). What We Talk About When We Talk About Indicators: Current Approaches to Human Rights Measurement. Human Rights Quarterly 23. https://www.jstor.org/stable/4489371?seq=1.
[234] Maréchal, Nathalie. (2015). Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate. International Journal of Communication 9. https://ijoc.org/index.php/ijoc/article/viewFile/3330/1494.
[235] Maréchal, Nathalie. (2015). Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate. International Journal of Communication 9. https://ijoc.org/index.php/ijoc/article/viewFile/3330/1494.
[236] Remensperger, John, Laura Schwartz-Henderson, and Kristina Cendic. (2018). Using Research in Digital Rights Advocacy: Understanding the Research Needs of the Internet Freedom Community. Internet Policy Observatory. https://www.asc.upenn.edu/sites/default/files/2021-02/using-research-in-digital-rights-advocacy-internet-policy-observatory.pdf
[237] KII 17
[238] Remensperger, John, Laura Schwartz-Henderson, and Kristina Cendic. (2018). Using Research in Digital Rights Advocacy: Understanding the Research Needs of the Internet Freedom Community. Internet Policy Observatory. https://www.asc.upenn.edu/sites/default/files/2021-02/using-research-in-digital-rights-advocacy-internet-policy-observatory.pdf
[239] Maréchal, Nathalie. (2015). Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate. International Journal of Communication 9. https://ijoc.org/index.php/ijoc/article/viewFile/3330/1494.

[240] KII 17
[241] KII 12
[242] KII 13
[243] KII 6
[244] KII 12
[245] KII 17
[246] FGD 6
[247] KII 12
[248] KII 12
[249] KII 12
[250] KII 6
[251] KII 8
[252] FGD 6
[253] FGD 6