Working Paper

Portfolio Assessment of Department of State Internet Freedom Program: An Annotated Briefing

Ryan Henry, Stacie L. Pettyjohn, Erin York

RAND National Security Research Division

WR-1035-DOS

February 2014

Prepared for the U.S. Department of State, Bureau of Democracy, Human Rights, and Labor

RAND working papers are intended to share researchers' latest findings and to solicit informal peer review. This paper has been approved for circulation by the RAND National Security Research Division but has not been formally edited or peer reviewed. RAND working papers can be quoted and cited without permission of the author provided the source is clearly referred to as a working paper. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

Preface

This research was conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis on defense and national security topics for the U.S. and allied defense, foreign policy, homeland security, and intelligence communities and foundations and other nongovernmental organizations that support defense and national security analysis.

For more information on the International Security and Defense Policy Center, see http://www.rand.org/nsrd/ndri/centers/isdp.html or contact the director (contact information is provided on the web page).

Comments or questions on this annotated brief/working paper should be addressed to the project leader, Ryan Henry, at rhenry@rand.org. This working paper will be developed into a completed RAND report soon.

Abstract

RAND researchers conducted an assessment of the State Department's Bureau of Democracy, Human Rights, Labor (DRL) Internet freedom portfolio for Fiscal Year 2012-13. Applying an analytical methodology employing both multi-attribute utility analysis and portfolio analysis techniques, the assessment showed good alignment between State's strategy and the cumulative effect of the eighteen funded projects. Additionally, the portfolio was assessed to be well balanced with an unrealized potential for supporting emergent State Department needs in enlarging political space within authoritarian regimes. We found that the investment in developing Internet freedom capacity and capabilities would likely have residual value beyond the portfolio's funded lifespan, with positive, but indirect, connections to civic freedom. Moreover, promoting Internet freedom appears to be a cost-imposing strategy that simultaneously aligns well with both U.S. values and interests, pressuring authoritarian rivals to either accept a free and open Internet or devote additional security resources to control or repress Internet activities. Finally, it was assessed that the value of such analysis is best realized over multiple stages of the portfolio's lifecycle.

Table of Contents

Preface ii
Abstract ii
Figures iv
Summary v
  Methodology v
Acknowledgments vii
Abbreviations viii
Findings 1
  Performance 1
  Balance 1
  Synergy 2
  Additional Observations 3
    Technology 3
    Enduring Value of Portfolio 3
    Risk 4
    Project Execution 4
    Common Challenges 4
    Internet Freedom Linkage to Enlarged Political Space 5
    Internet freedom As a Cost-Imposing Strategy 6
  Conclusions 6
Background and Methodology 10
Performance 22
Balance and Diversity 34
Synergy 39
Additional Observations 45
Findings, Recommendations, and Conclusions 58
Bibliography 62

Figures

Figure 1: Optimizing Synergy Framework for Internet Freedom Portfolio 2
Figure 2: Nested Measures Constitute Total Performance 18
Figure 3: Modified Delphi Method..... 20

Summary

The United States has long argued that all people have a fundamental right to freely express and share their ideas. [1] Because the Internet enables individuals to communicate independent of time or distance, it facilitates the free flow of information. Yet some repressive states attempt to limit the content available online and use the Internet to identify and track those who oppose their rule. The State Department's Bureau of Democracy, Human Rights, and Labor (DRL) Internet freedom program seeks to counter the efforts of authoritarian regimes to censor and control the Internet.[2] DRL sponsored RAND in an assessment of their Internet freedom program's portfolio of eighteen specific projects funded in the FY 2012-13 timeframe in order to determine its effectiveness regarding portfolio performance, balance, and synergy among projects.[3]

Methodology

To assess DRL's Internet freedom portfolio, RAND researchers employed a multi-attribute utility analysis and the Portfolio Analysis and Management Method (PortMan).[4] We began by developing an Internet freedom model that identified the variables which influence whether an individual chooses to use the Internet to expand political space. From this model, we created a set of metrics that formed the basis of the value, cost, and risk scores which determined the overall portfolio's performance. One challenge was turning qualitative inputs into standardized quantitative metrics that could be evaluated by the PortMan methodology. To do this, RAND researchers built a survey protocol to ensure that its interviews of the DRL grantees were standardized and replicable. The protocol captured qualitative data fields for a multi-attribute utility analysis of projects: including their background, desired outcomes, specific outputs, implementation methodology, execution alignment with key Internet freedom attributes, cross-project synergy, tool employment, measures of performance achievement and measure of

[1] Dickinson, Elizabeth, "Internet Freedom: The Prepared Text of U.S. Secretary of State Hillary Rodham Clinton's Speech, Delivered at the Newseum in Washington, D.C.," *Foreign Policy,* January 21, 2010.

[2] Daniel Baer, Baer, Daniel, Deputy Assistant Secretary, Bureau of Democracy, Human Rights, and Labor, "Promises We Keep Online: Internet Freedom in the Organisation for Security and Cooperation in Europe (OSCE) Region," Statement Before the Commission on Security and Cooperation in Europe (U.S. Helsinki Commission), Washington, D.C., July 15, 2011.

[3] RAND Response to RFP DRL-11-RFP-01-INTERNET-110307, 31 March 2011

[4] Alan A. Lewis, *The Use of Utility in Multiattribute Utility Analysis*, Santa Monica, Calif.: RAND Corporation RAND Paper P-6396, , RAND, Santa Monica, 1980; and Eric Landree, Richard Silberglitt, Brian G. Chow, Lance Sherry, and Michael S. Tseng, *A Delicate Balance: Portfolio Analysis and Management for Intelligence Information Dissemination Programs*, Santa Monica, Calif.: RAND Corporation, MG-939, 2009.

effectiveness relevance, technical, programmatic, and acceptance risk, among others. After collecting the qualitative data through semi-structured interviews, we then relied on a small group of experts and an approach that facilitates consensus building to estimate the value, risk, and cost metrics for each project. The resulting data was then analyzed using the PortMan framework to determine the overall portfolio's performance and balance.

Acknowledgments

The authors thank Ian Schuler, Chris Riley, Betsy Bramon, and Stephen Schultze from the Department of State for their valuable feedback and guidance on this study. At RAND, we gratefully acknowledge the help of our colleagues Oleysa Tkacheva and Christina Bartol. Finally, we thank our internal reviewers, Andrew Morral and Sasha Romanosky, for their helpful comments.

Abbreviations

BBG	Broadcasting Board of Governors
DARPA	Defense Advanced Research Projects Agency
DRL	Bureau of Democracy, Human Rights, Labor, U.S. Department of State
FY	fiscal year
GOR	grant officer representative
IP	internet protocol
IT	internet technology
ITU	International Telecommunications Union
NGO	non-governmental organization
PortMan	Portfolio Analysis and Management Method
QOS	quality of service
USAID	United States Agency for International Development
USG	U.S. government
VPN	virtual private network

Findings

Performance

The Internet freedom portfolio assessment was based on the cumulative performance value of individual projects within the portfolio. The Internet freedom performance value of the individual projects was determined by each project's overall contributions to four major variables that impact Internet freedom and political space: 1) access to the Internet, 2) anonymity and security when accessing the Internet, 3) awareness and understanding of security threats and protective measures, and 4) advocacy for ensuring a free and open Internet compatible with the aforementioned U.S. policy toward free speech and human rights online. A project's risk level and cost, both direct and indirect, to the U.S. government also influenced its portfolio contribution.

Under this methodology, the highest performing projects were active in multiple areas of Internet freedom at comparatively low risk and cost. The DRL program strategy emphasized anonymity when using the Internet as a key component, and viewed advocacy as a less essential input. The PortMan formula used to calculate performance reflected DRL's strategy. Consequently, projects that focused primarily on advocacy had relatively low performance scores. Conversely, projects that made a key contribution to anonymity on the Internet were among the higher performers.

In a broad sense, this assessment of the overall portfolio found a strong diversity of effort and balance across the four Internet freedom variables. Each of the four performance aspects was addressed by multiple projects, a dispersion that adds robustness to the portfolio, given the challenges in measuring direct impacts in this area. Additionally, there was a clear connection between DRL's stated program objectives and the projects' objectives and lines of effort.

Balance

The performance assessment revealed that the DRL Portfolio was balanced in the Internet freedom area with respect to project focus and geographical distribution. The quantitative assessment revealed that projects cluster into five functional types: technology development, training, technology testing, advocacy, and mixed efforts. The portfolio also incorporates a mix of high-risk and high-gain projects, along with some implementers who use more established approaches. All funded projects were clearly aligned with Internet freedom objectives, but the projects varied substantially on approach, breadth, geo-political focus, and investment allocation.

Although "The Onion Router" (Tor) project, a circumvention technology based on proxy routing, is not a direct DRL grantee, it was employed by several projects within the DRL

portfolio. Nine of the DRL projects used Tor to some extent, with most deriving a benefit in the access and anonymity components of Internet freedom.

Synergy

A key finding from the portfolio assessment was that the total impact of the program is greatly enhanced by the interaction and collaboration between implementers. Projects from the five above cluster areas intersect within the portfolio and produce opportunities for project synergy that can lead to enhanced project, as well as portfolio, performance or additional collaboration beyond the scope and timeframe of the DRL grant. The potential benefit of this element is substantial: projects engaging in technology development will benefit from interaction with groups testing that technology for security flaws; training programs may distribute newly developed circumvention tools, etc. as illustrated in the Figure 1 below.

Figure 1: Optimizing Synergy Framework for Internet Freedom Portfolio

RAND researchers mapped the existing relationships among DRL's projects to identify the level of synergy currently in DRL's Internet freedom portfolio. This analysis revealed that many projects informally cooperated or formally collaborated with other DRL grantees, but that these connections were largely ad hoc and based on preexisting personal and professional relationship. We also found that Tor was utilized by a number of DRL projects and produced an added element of synergy. While there are some connections among DRL grantees, more networking would be valuable in realizing the portfolio's full synergy potential. DRL, therefore, should continue to enhance and encourage their grantees to establish mutually beneficial connections through a number of low-cost actions.

There is an inherent tension between cooperation and competition in a limited resource environment, but DRL could address this challenge in their selection criteria. Synergy presents an especially worthwhile investment because of its low cost and high potential payoff. Even if projects do not immediately collaborate, the latent relationships facilitated by DRL may produce lasting value. In particular, by fostering personal and organizational ties and enhancing trust, the Internet Freedom community would be positioned to organically and rapidly respond to rapidly developing Internet freedom-associated crises.

Additional Observations

Technology

Developing new technologies that enable individuals to have unfettered and secure access to the Internet is a significant but complicated part of the DRL portfolio. The struggle between those promoting Internet freedom and those trying to control and censor the Internet is a fast-paced cat and mouse game. Consequently, the speed of this contest often outstrips the grant cycle, and implementers often have to modify their proposed deliverables in response to developments on the ground. Responding effectively to the countermoves made by authoritarian governments is difficult under any circumstances. This predicament is further complicated by the fact that technology development is not a traditional State Department activity and, therefore, not one of its core capabilities. Partnering with other U.S. government entities who have proven technology development infrastructure could potentially help to overcome this limitation.

While developing technology—both through evolutionary improvements to existing circumvention and anonymity tools or the incubation of new revolutionary Internet freedom capabilities—is a critical component of DRL's Internet freedom portfolio, it alone cannot produce a free and open Internet. There is not a purely technical solution that would guarantee Internet freedom. Instead it is a political struggle that takes places in many different arenas, including legislatures, courts, and international organizations, and therefore, requires a multi-faceted response.

Enduring Value of Portfolio

DRL's investment in Internet freedom should have enduring value that extends well beyond the life of the individual grants. In particular, one of the most important effects of the DRL portfolio appears to be the community it nurtures. Although more might be done, DRL has taken steps to maximize the return on its Internet freedom portfolio by bringing together the individuals, organizations, and tools it supports. The DRL Internet freedom community could play different roles at different times. Typically, the DRL Internet freedom community is focused on increasing the State Department's steady-state capability to promote freedom online by encouraging formal and informal collaboration between grantees to improve the efficacy of both projects. At the same time, fostering these ties also develops a latent surge capacity to respond during Internet freedom-associated crises. At critical moments, the DRL-sponsored community has the capacity to rapidly and independently respond to developments in an effort to expand political space. In these circumstances, a self-synchronizing community comprised of independent actors whose interests are aligned with the United States government is not only well-positioned to react, given its grassroots connections, but it also is more agile and capable of responding in a timely fashion than the government. Moreover, by having the U.S. Government stay in the background, it reduces the potential for blowback.

Risk

This portfolio assessment included investigation of three major types of risk: performance/management, political, and an individual user's security. It did not address two types of risk—technical risk and the likelihood that circumvention technologies could be abused—because they were beyond the scope of this project.

Based on the early phase of most projects assessed, there were no current indications of program risks yet materializing. That does not mean that problems might not arise in the future. Additionally, individual projects appeared internally risk-sensitive. Political risk seemed well within the comfort zone of DRL. Throughout each of the projects that had interaction with Internet freedom activists from within authoritarian regimes, there was a heightened sensitivity to user security risk. Each project had protocols and policies to protect the exposure of its users from repressive and/or retaliatory actions by the regime.

One area where the portfolio appeared to accept risk was in the technology arena, specifically technology development risk. DRL's portfolio included apparently low- and high-risk technologies for development within the portfolio, which correlated closely with the evolutionary or revolutionary nature of the technology under development. We viewed DRL's failure-tolerance approach as both healthy for the technology development community and important for the advancement Internet freedom capabilities.

Project Execution

RAND researchers confirmed there were several key components that characterized well-run projects, principal among them: a staff that includes a visionary or idea champion, a skilled functional specialist, and a competent program manager. At times, one person might be responsible for all of these tasks, but more often projects had different people filling these roles. Another key component among the best projects was healthy interactions with other Internet freedom programs and the larger Internet freedom community, which helped them to realize their full potential.

Common Challenges

During the assessment, we found that many DRL implementers face a number of similar challenges. One of the most common problems encountered by grantees was the difficulty of securing and retaining skilled technologists at a non-profit organization's salary. Given that there are much more lucrative careers in the private sector, implementers had to search for qualified personnel with technical skills who were primarily motivated by the cause of advancing Internet freedom. While, fortunately, such dedicated tech-savvy individuals exist, their numbers are few and their talents highly sought.

Many of the projects were based on a compelling idea and dedicated staff, but not all projects had a sufficient cadre of experienced developers and managers to ensure their long-term success. Some lacked experience in negotiating the multi-stakeholder environment that characterizes the Internet freedom community.

Another issue many DRL implementers faced was finding ways to deal with rapidly changing circumstances or crises. At times, real-time developments raised new issues or challenges not addressed in the original grant. Implementers, therefore, desired for more flexibility, so they could modify their activities to respond to unforeseen opportunities to provide greater value.

Beyond Tor, one potential challenge area yet to be negotiated by any of the projects within the DRL portfolio is their ability to scale beyond pilot-project demonstrations. There are number common growth hurdles experienced by both for-profit and not-for-profit that will need to be overcome if any of these projects are to have anything beyond niche impact.

Internet Freedom Linkage to Enlarged Political Space

RAND researchers found, as part of a more theoretical research effort, that there is a positive, but indirect, relationship between Internet freedom and the expansion of political space in societies. Historically, there is an observable relationship between online and offline mobilization. The Internet has played an important role in the expansion of political space by eliminating distance and time as constraints to sharing information and building trust networks. Nevertheless, typically Internet freedom has not been a primary causal factor that directly increases political space. Instead it has acted as an accelerant to social movements, rather than a causal factor. DRL's projects seek to assure that all people have free access to the Internet, which could be a critical enabler that helps to empower opposition movements within repressive states.

Generally, there are two major tradeoffs an Internet freedom policy needs to balance: deepening versus broadening, and steady state versus crises. First, an Internet freedom strategy needs to ensure it targets both opinion leaders and the broader population. In other words, it needs to deepen by focusing on those who already desire Internet freedom (opinion leaders), but also broaden by drawing in the general populace to increase the number of people who are mobilized and politically active. Second, an Internet freedom strategy needs to find the appropriate balance between increasing individuals' ability to securely access that Internet every day, and intervening during crises when Internet freedom could potentially tip the balance towards greater political space.

Internet freedom As a Cost-Imposing Strategy

While Internet freedom is consistent with the U.S.'s ideological and economic interests, somewhat unusually, it also largely aligns with the U.S.'s national security interests.[5] Equally important, by investing relatively little in Internet freedom (approximately $30 million a year) initiatives, the United States can impose costs on authoritarian rivals who are forced to devote significantly more resources to maintaining domestic stability.[6] Cost-imposing strategies take actions that pressure rivals to implement disproportionately costly countermeasures. Many current and potential authoritarian competitors, such as Iran and China, face endemic domestic tensions that center on a lack of freedom and regime legitimacy issues. As a result, both Tehran and Beijing have emphasized preserving domestic stability above all other goals. In short, promoting Internet freedom capitalizes on traditional American strengths and simultaneously exploits the enduring weaknesses of authoritarian rivals by compelling repressive regimes to spend ever greater sums to preserve their rule. In an age of fiscal austerity and the growing economic prowess of potential adversaries, it is particularly important that the United States rely on policies, like Internet freedom, that have a favorable cost-exchange ratio.

Conclusions

In summary, we assessed DRL's Internet freedom portfolio as balanced and of benefit to the U.S. interests and values. Analysis of the portfolio of projects showed them to be properly targeted and executed. The overall contribution of the portfolio, if properly developed, should increase in the future. The portfolio assessed appeared to be balanced, with a healthy mix of projects in both their objectives and approaches. Risk within the portfolio seemed appropriate and prudent, with a suitable degree of failure-tolerance spread across the portfolio.

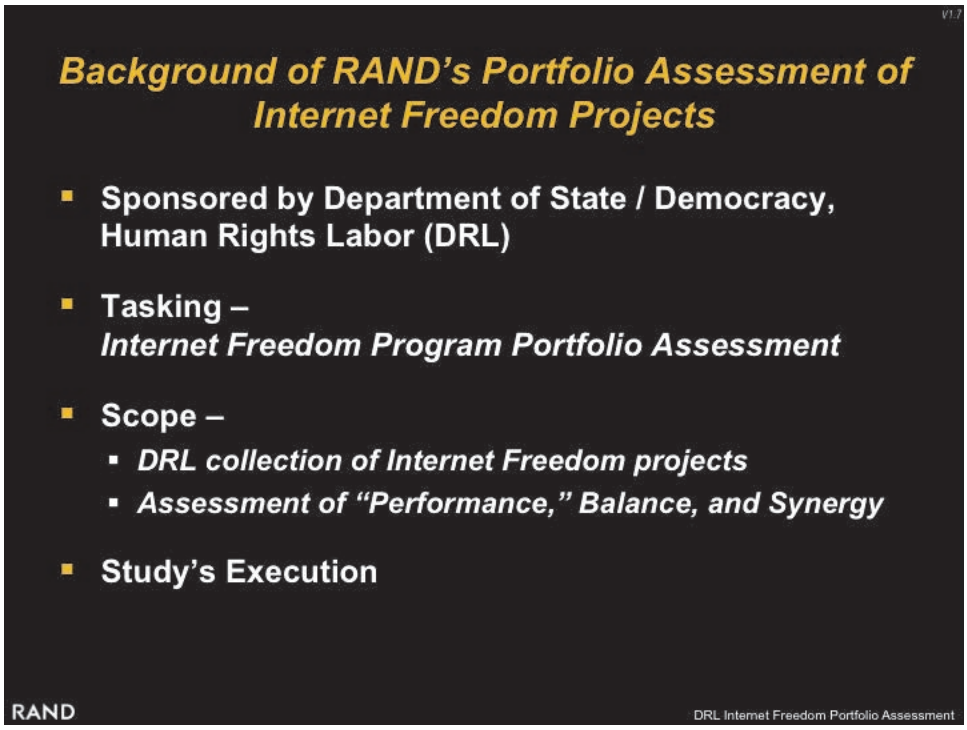
There are clear indications that Internet freedom has a positive, but indirect, connection to enlarging political space within repressive regimes. Internet freedom initiatives have the potential to be a high-leverage national security tool for democratic open societies, with cost-imposing characteristics vs. authoritarian regimes.

We recommend that DRL consider: some form of contingency resourcing for the application of developed Internet freedom capabilities for rapid application to real-world pop-up crises, the development of a *Best Practices* clearing house for implementers and the broader Internet freedom community, and continued longitudinal assessment of the portfolio as old projects complete and new projects are begun

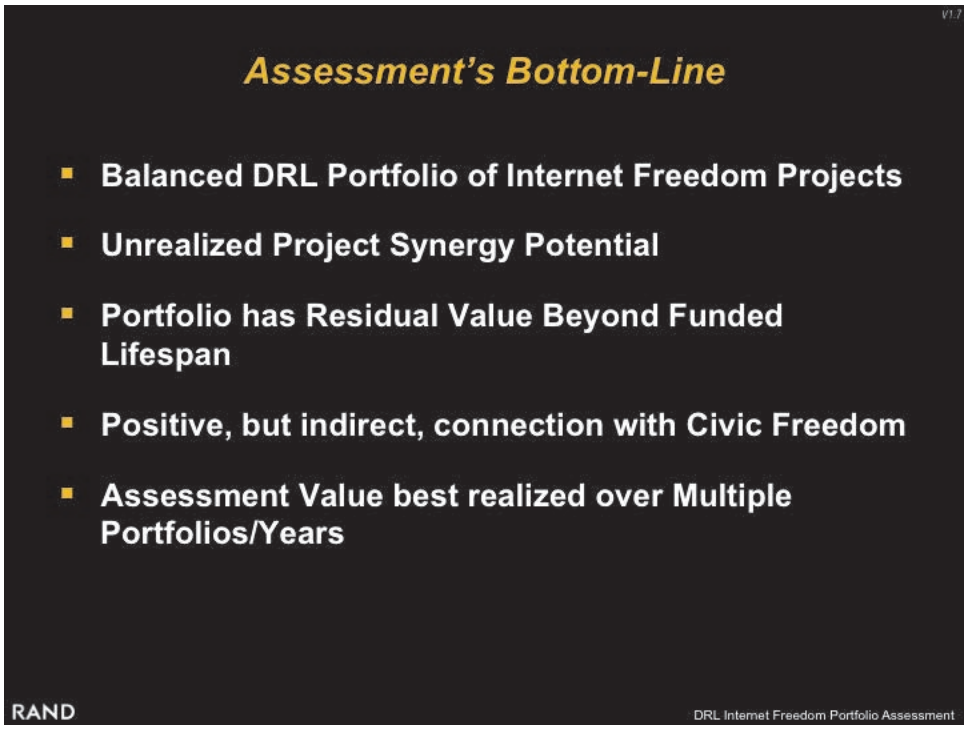
---

[5] Internet freedom can help the United States to compete against authoritarian rivals. Nevertheless, there is a tension between Internet freedom and other security concerns, particularly terrorism, which the Snowden revelations about the NSA surveillance program revealed.

[6] This figure only includes the State Department, USAID, and the BBG. Patricia Moloney Figliola, Kennon H. Nakamura, Casey L. Addis, and Thomas Lum, *U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology*, Washington, D.C.: Congressional Research Service, January 3, 2011., p. 16.



RAND researchers conducted an assessment of the State Department's Bureau of Democracy, Human Rights, Labor (DRL) Internet freedom portfolio for Fiscal Year 2012-13. Employing both multi-attribute utility analysis and portfolio analysis techniques, the assessment showed good alignment between DRL's strategy and the cumulative effect of the eighteen funded projects. To assess DRL's Internet freedom portfolio, we collected information on each grantee through a semi-structured interview. The portfolio was then judged on three different metrics: performance, balance and synergy. Performance indicates the value of the portfolio but also its risk and cost. For balance, we considered the type of projects that DRL funded, the geographic distribution of its projects, and the level of risk across the portfolio. Synergy refers to links between different grantees and explores whether the projects are working together to increase the performance of the overall portfolio.



In short, our assessment concluded that DRL's Internet freedom portfolio of projects is balanced between the development of new technologies that enable individuals to circumvent Internet filters or protect an individual's identity; training programs that inform individuals about their vulnerabilities and teach them how to minimize their risk while online; advocacy programs that de-legitimize Internet censorship, promote a multi-stakeholder model of Internet governance, teach individuals to use the Internet to achieve political objectives, or assist activists in extremis; testing and evaluation projects that assure that the circumvention tools that DRL is funding are of high quality and do not have critical vulnerabilities; and mixed projects that are involved in multiple different areas. Nevertheless, there is room for improvement, especially in terms of enhancing synergy within the portfolio. The Internet freedom community that DRL nurtures is potentially one of the most important and enduring outcomes because it is likely to have considerable value beyond the portfolio's funded lifespan. Therefore, DRL should continue to prioritize fostering connections between its grantees. Additionally, there is a positive, but indirect, connection between DRL's Internet freedom portfolio and the expansion of civic freedom within authoritarian regimes. Alone access to the Internet is unlikely to produce popular revolutions that overthrow authoritarian regimes and result in the establishment of liberal democracies, but unfettered and secure Internet access is a critical enabler and accelerant that can help to achieve these objectives. Finally, it was determined that the value of such analysis is best realized over multiple stages of the portfolio's lifecycle. While this one-time assessment represents an accurate snap-shot at a particular moment-in-time, understanding the full value of the DRL portfolio, and possible areas of concern, calls for periodic assessment over time to

validate its findings. This is particularly important given the fact that Internet freedom is a relatively new programmatic area as well as a rapidly changing environment.

The remainder of this report is divided into six sections. The first section discusses background about Internet freedom and explains the methodologies employed to assess DRL's Internet freedom portfolio. The second section examines how DRL's Internet freedom portfolio performed on several different dimensions. The third and fourth sections assess the portfolio balance and synergy respectively. The fifth section incorporates some additional observations and lessons learned from the assessment. The final section presents the findings, conclusions, recommendations.

Currently, there is a struggle between those who want to communicate freely and securely and those who seek to restrict the content available online and control the Internet. New communications technologies have converted the Internet from a static vehicle for consuming information into an interactive cyber community, the so-called "Web 2.0."[7] The Internet is increasingly dominated by social media platforms and tools that enable users to produce online content, to interact with others, and to coordinate their actions. As social media sites—which include microblogging, social networking, photo and video sharing, social news, and virtual gaming websites—have proliferated, it has created new opportunities for collaboration and mass mobilization.[8] While most people use Web 2.0 sites as a diversion, these online platforms can also strengthen civil society by spreading information and encouraging debate. Additionally,

[7] Sarah Joseph, "Social Media, Political Change, and Human Rights," *Boston College International and Comparative Law Review*, Vol. 35, No. 1, January 1, 2012, pp. 145-150.

[8] Microblogging sites include Twitter and Sina Weibo. Examples of social networking sites are Facebook and MySpace. Instagram is a hybrid photo and video sharing and social networking website. Other image sharing sites include YouTube and Flickr. Social news sites, such as Reddit and Digg, contain user posted stories and allow users to rank the popularity of these stories and to comment on them. Virtual gaming websites include the World of Warcraft and EverQuest.

social media can be used as a coordinating tool, helping groups to overcome collective action problems and ultimately to effect social and political change.[9]

The ability of social media to empower people was dramatically illustrated during the Arab Spring uprisings of 2011 and 2012. In Tunisia, for example, the self-immolation of a young street vendor sparked demonstrations in the town of Sidi Bouzid. Tunisian protestors used cell phones to capture photos and videos of the brutal police response which were then posted on Facebook and YouTube. Because Tunisia had a relatively high rate of Internet penetration, these images rapidly spread across the nation, galvanizing citizens who were outraged by their government's brutality, corruption and incompetence to stage additional protests.[10] Eventually more than 2 million Tunisian members of Facebook changed their profile picture to read "Ben Ali dégage!" (Ben Ali Get Out!).[11]

At the same time, states can use the Internet to monitor and control their citizens. Some critics argue that the Internet and social media do not inevitably spread democracy (as the Arab Spring uprisings have demonstrated), but instead help to entrench authoritarian regimes.[12] According to this view, the Internet is a tool for repression because it enables governments to more cheaply and easily restrict their citizens' freedoms, locate and track down protesters, and spread their own propaganda. For example, supporters of Bashar al-Assad have reportedly launched phishing attacks against regime opponents to identify dissidents and infiltrate their networks.[13] The Internet, therefore, is not inherently emancipatory, but can also increase oppression.

Recognizing that "modern information networks…can be harnessed for good or ill" and that "a new information curtain" had descended "across much of the world," in January 2010 former Secretary of State Hillary Clinton announced that the "we stand for a single Internet where all of humanity has equal access to knowledge and ideas." Clinton also pledged that the United States would work to ensure that "these technologies" are "a force for real progress in the

---

[9] Clay Shirky, "The Political Power of Social Media: Technology, the Public Sphere, and Political Change," *Foreign Affairs*, Vol. 90, No. 1, January/February 2011, p. 29; Eric Schmidt and Jared Cohen, "The Digital Disruption: Connectivity and the Diffusion of Power," *Foreign Affairs,* Vol. 80, No. 6, November/December 2010; Joseph, 2012, pp. 152-156.

[10] Sanja Kelly, Sarah Cook, eds., *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media,* Washington, D.C.: Freedom House, April 18, 2011, pp. 322-323.

[11] Marc Lynch, *The Arab Uprising: The Unfinished Revolutions of the New Middle East*, New York, N.Y.: PublicAffairs, 2013; Laryssa Chomiak and John P. Entelis, "The Making of North Africa's Intifada," in David McMurray and Amanda Ufheil-Somers, eds., *The Arab Revolts: Dispatches on Militant Democracy in the Middle East*, Bloomington, Ind.: Indian University Press, 2013, p. 46.

[12] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom,* New York, N.Y: PublicAffairs, 2011*;* Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, New York, N.Y.: Basic Books, 2012.

[13] Eva Galperin and Morgan Marquis-Boire, "Syrian Activists Targets with Facebook Phishing Attack," *Electronic Frontier Foundation*, March 29, 2012.

world."[14] The State Department's Bureau of Democracy, Human Rights, and Labor (DRL) Internet freedom program awards grants to groups that are trying to advance Internet freedom by countering censorship, developing secure ways to communicate, providing digital safety training, conducting research on the effects of Internet freedom and Internet repression, and directly supporting activists on the front lines of the struggle against authoritarian regimes.[15]

[14] Dickinson, 2010.

[15] U.S. Department of State, *Internet Freedom*, undated; Baer, 2011.

DRL sponsored RAND in an assessment of their Internet freedom program's portfolio of eighteen specific projects funded in the fiscal year 2012-13 timeframe in order to determine its effectiveness regarding portfolio performance, balance, and synergy among projects.[16] These projects were in various stages as two were just beginning, while sixteen were in the middle of executing their tasks when they were interviewed. Due to concerns about the security of those working on or participating in these efforts, we agreed not to reveal any information about the specific projects. The U.S. government has awarded Internet freedom grants since the early 2000s. Initially, most USG-sponsored efforts were focused on helping individuals to bypass firewalls in societies like China and Iran.[17] Since 2008, the Department of State has broadened its program by funding Internet freedom as a part of its global human rights agenda with the goal of "ensur[ing] that any child, born anywhere in the world, has access to the global Internet as an open platform on which to innovate, learn, organization, and express herself free from undue interference or censorship."[18] Consequently, in addition to circumvention technologies, DRL now funds programs that enable secure communications and protect privacy, offer digital safety training, shape international norms about the Internet, monitor and research the state of Internet

[16] The eighteen projects within DRL's 2012 portfolio were in various stages with some just beginning, while others were nearing their completion. The methodology dealt with this fact by assigning greater uncertainty scores to the projects that were in their initial phase. Because more advanced projects had made more progress, there was less uncertainty associated with whether they would be able to complete their deliverables.

[17] Thomas Lum, *China, Internet Freedom, and U.S. Policy,* Washington, D.C.: Congressional Research Service, July 13, 2012, p. 12.

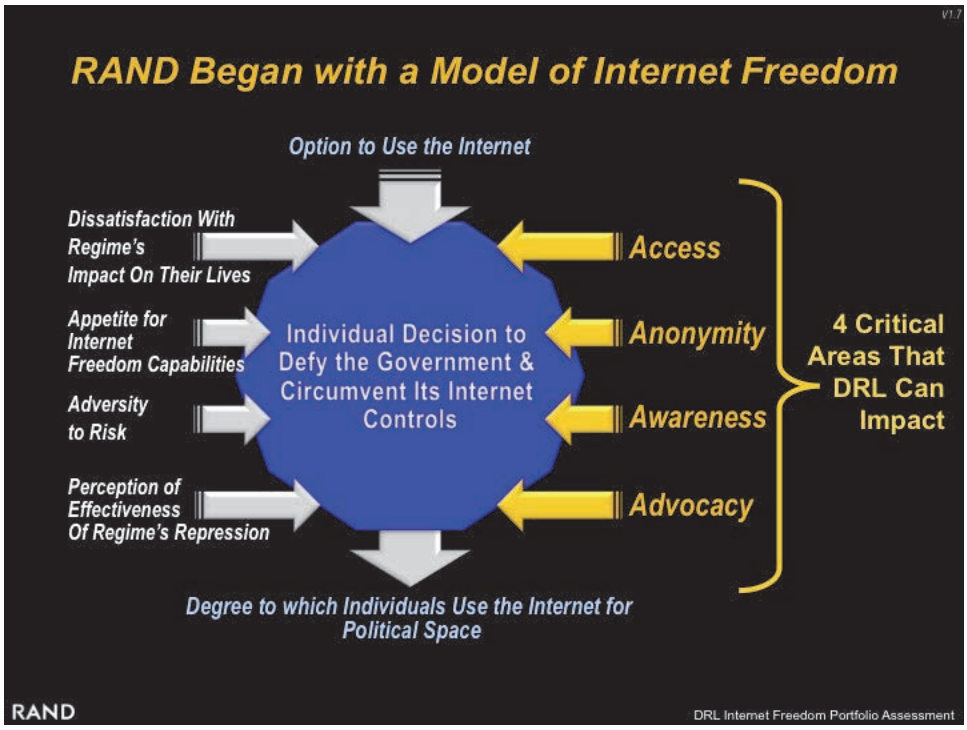
[18] U.S. Department of State, *Internet Freedom*

freedom globally, and generally promote policies that preserve the open character of the Internet.[19]

In conducting this assessment, there were a number of challenges. Most notably, Internet freedom is a relatively new area, which meant that we had to develop from the ground up a method for assessing DRL's portfolio. Moreover, due to the diversity of DRL's Internet freedom portfolio as well as the nature of the programs, there are not easily accessible or meaningful quantitative metrics for measuring the value of these projects. For example, collecting project data could jeopardize their users' security. To overcome these hurdles, we developed an Internet freedom model, and used a multi-attribute utility analysis as well as a portfolio balancing tool.

The main objective of this assessment was to determine if DRL had developed a robust portfolio of programs resourced through appropriated funds that were in line with its overarching strategy. To gather information on the eighteen projects, we conducted interviews with each of the grantees and examined supporting materials, such as quarterly reports. The interviews covered a range of topics, including the project's background and objectives, its various lines of efforts, its programmatic execution, deployment strategy, credentials of the staff, and measures of performance. It was agreed with DRL that it would be beyond the scope of this project to measure the actual impact of these programs (e.g. test the technology, gauge what trainees actually learned), but we did evaluate the execution of the projects and assessed whether they were hitting their cost, schedule, and performance targets (e.g. in terms of number of individuals trained, lines of code written, or launching a new website, etc.) that they had outlined in their statement of work.

[19] Lum, 2012, pp. 12-13; Fergus Hanson, *Baked In and Wired: eDiplomacy@State*, Washington, DC: Brookings, October, 25, 2012, p. 26.



Our first task was to develop an Internet freedom model that captured the factors that influence whether a citizen in a repressive state decides to use the Internet to try to expand the political space in his or her society.[20] In general, research has found that "the power of civil society is strengthened through higher levels of connectivity, unfettered access to knowledge, freedom of expression, and freedom to engage in collective action facilitated by digital tools: in short, the creation of social capital online."[21] Yet an individual decides whether to use the Internet for simply entertainment or communication or to achieve some sort of political objective. Our Internet freedom model is based on the assumption that individuals are essentially rational decision-makers, meaning they consider the likelihood of realizing expected costs and benefits before acting and select the course of action that offers the highest expected payoff.[22] When creating this model, we recognized that many of the factors that guide an individual's decision calculus are beyond the influence of the U.S. government. For example, one of the

[20] Political space consists of the freedom to assemble, free speech, and the ability to select a state's leaders through free and fair elections. Political space expands when people exercise these rights. Olesya Tkacheva, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini, and Caroline Baxter, *Internet Freedom and Political Space*, Santa Monica, Calif.: RAND Corporation, RR-295-DOS, 2013, pp. 4-5.

[21] Robert Faris and Rebekah Heacock, "Introduction," in Urs Gasser, Robert Faris, Rebekah Heacock, *Internet Monitor 2013: Reflections on the Digital World*, Cambridge, Mass.: Berkman Center for Internet and Society, December 12, 2013, p. 1.

[22] For more on rationality see Jon Elster, ed., *Rational Choice*, New York, N.Y.: NYU Press, 1986. We realize that people are not perfectly rational and that misperception can often interfere with the pursuit of utility maximization. Nevertheless, it is very difficult to theorize about or predict misperception because they are often intimately linked to an individual's traits and experiences. For more on misperception see Robert Jervis, *Perception and Misperception in International Politics*, Princeton, NJ: Princeton University Press, 1976.

critical contextual factors is the level of Internet penetration within a state.[23] A key precondition, therefore, is that a state has sufficient communications infrastructure in place that citizens can go online. Additionally, there are other variables that may be influenced by a combination of things that are difficult to directly effect. An individual's dissatisfaction with a repressive government, for example, is probably a product of one's particular situation as well as personality.[24] Unhappiness with the regime is a necessary condition for an individual to use the Internet to try to increase openness in their state. Similarly, a person's level of risk acceptance and their appetite for Internet freedom capabilities are likely to be strongly influenced by their individual disposition. Some people are more willing to take dangerous actions, while others are more concerned about the potential negative repercussions and tend to avoid activity that could jeopardize their personal wellbeing.[25] An individual's predisposition to seek out Internet freedom technologies is probably tied to one's exposure to and general comfort with technology.[26] This in turn could also be related to age or many other individual traits, and therefore, falls outside of the realm of what the U.S. government can directly impact. Finally, an individual's willingness to take the risky step of online activism will depend in part on that person's perception of whether the regime is willing and capable of punishing him or her for this action.[27]

Although there are many variables that are outside of the control of the U.S. government, there are a number of critical factors—in particular access, anonymity, awareness, and advocacy—that are amenable to manipulation. First, an individual is unlikely to be able to use the Internet to expand political space, if he or she does not have access to the Internet. As mentioned above, Internet access requires infrastructure, but even if one can easily get online, many states still try to constrain access by blocking or filtering websites that considered to be unacceptable. For example, some states, like China, use automated filtering systems to limit the online content that their citizens can view.[28] At other times, a government may try to restrict

---

[23] For various metrics on Internet penetration worldwide see: International Telecommunications Union, *The World in 2013: ICT Facts and Figures*.

[24] Dissatisfaction or popular discontent is necessary, but far from sufficient to explain activism or outright rebellion. Mark I. Linbach*, The Rebel's Dilemma*, Ann Arbor, Mich.: University of Michigan Press, 1998, p. 283. For more on discontent see Ted Robert Gurr, *Why Men Rebel?: Fortieth Anniversary Edition*, Boulder, Colo.: Paradigm Publishers, 2011.

[25] Varying risk acceptance has been show to impact likelihood of collective action. Werner Raub and Chris Snijders, "Gains, Losses, and Cooperation in Social Dilemmas and Collective Action: the Effects of Risk Preferences," *Journal of Mathematical Sociology*, Vol. 22, No. 3, 1997, pp. 263-302.

[26] See similar research on why people use the Internet and why some choose not to go online. Kathryn Zickuhr, *Who's Not Online and Why*, Pew Research Center, September 25, 2013. See also Phys.org, "Factors Identified that Influence Willingness to Use Technology," March 8, 2013; and Edward D. Conrad, Michael D. Michalisin, and Steven J. Karau, "Measuring Pre-Adoptive Behaviors Toward Individual Willingness to Use IT Innovations," *Journal of Strategic Innovation and Sustainability*, Vol. 8, No. 1, June 2012, pp. 81-92.

[27] Mancur Olson, "The Logic of Collective Action in Soviet-Type Societies," *Journal of Soviet Nationalities*, Vol. 1, No. 2, Summer 1990, p. 16.

[28] Robert Faris and Nart Villeneuve, , "Measuring Global Internet Filtering," in John Palfrey, et al., eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, Mass.: MIT Press, 2008; and Jonathan

access to information and online communications by shutting down or dramatically throttling the speed of Internet connections.[29] Unfettered access to the Internet helps individuals to spread information about injustices within their state, to communicate with others, and to coordinate their actions.[30] In short, access is key factor that influences whether one can use the Internet to expand political space.

Second, individuals are more likely to be politically active online if the government cannot easily identify and punish them. Yet government surveillance of the Internet is on the rise.[31] An ever growing number of countries are monitoring online activity at Internet choke points, like Internet exchanges and Internet Service Providers.[32] This is particularly important for non-democratic states that rely upon coercion to stay in power and monitor a variety of online platforms including mobile phone calls, text messages, email, browsing histories, voice over IP calls, and instant messages to control political opposition. Consequently, it is critical to protect the anonymity of online activists.

Third, digital activists are unlikely to be effective if they are not aware of their vulnerabilities to online surveillance, or if they lack knowledge about basic digital safety practices. Technologies that provide secure access to the Internet are essential, but they are useless if their intended users to do not know how to properly employ these circumvention and anonymity tools. Therefore, an important way to facilitate online activism is by expanding awareness of how a state can monitor online activities and sharing principles for reducing one's exposure to surveillance particularly by employing anonymity tools.

Finally, the U.S. government can support advocacy programs to teach people how to exercise their basic rights, to de-legitimize online censorship, to assist activists who are being prosecuted by a repressive state, and to campaign for a multi-stakeholder model of Internet governance. Trends suggest that the battle for Internet freedom is increasingly being waged in legislatures, courts, and international institutions.[33] Passing laws that criminalize online speech or hold intermediaries liable for the content posted on their websites is actually a more insidious way of stifling online freedom because it encourages self-censorship. Beijing, for example, has

---

Zittrain and John Palfey, "Internet Filtering: The Politics and Mechanisms of Control," in Palfrey et al., 2008, p. 32.

[29] Collin Anderson, "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran," June 18, 2013.

[30] Shirky, 2011, p. 31.

[31] Sanja Kelly, "Despite Pushback Internet Freedom Deteriorates," in Sanja Kelly et al., *Freedom on the Net 2013: A Global Assessment of Internet and Digital Media*, Washington, D.C.: Freedom House, 2013, pp. 7-9; Sanja Kelly, Sarah Cook, Mai Truong, eds., *Freedom on the Net 2012: Global Assessment of Internet and Digital Media, Washington, D.C.: Freedom House, 2012,* p. 10; Reporters Without Borders, *Enemies of the Internet 2013 Report: Special Edition Surveillance,* Paris, France, 2013.

[32] Ronald Diebert and Rafal Rohozinski, "Beyond Denial: Introducing Next Generation Information Access Controls," in Ronald Deibert, et al., eds, *Access Controlled: The Shaping Power, Rights, and Rule in Cyberspace*, Cambridge, Mass.: MIT Press, 2010, p. 9.

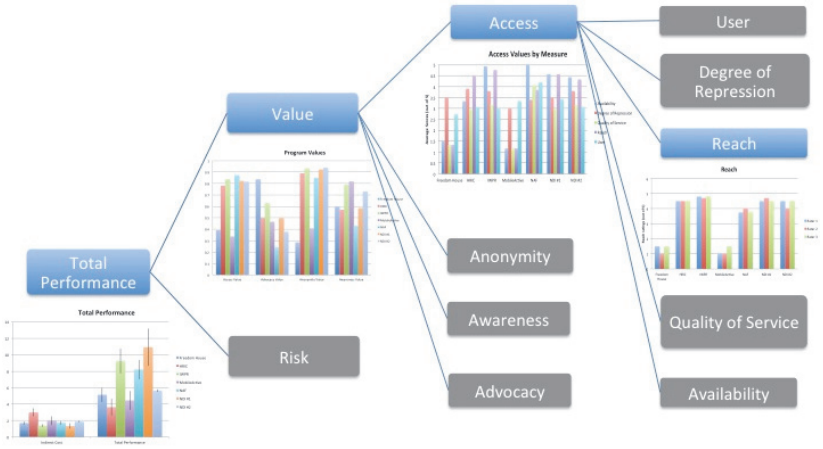
[33] Faris and Heacock, 2013, p. 8; Kelly, 2013, pp. 9-12.

created a climate of fear by requiring real-name registration (through identification cards with embedded computer chips) at Internet cafes and for a number of popular websites, like the microblogging platform Sina Weibo.[34] Increasingly governments are also arresting people, and handing out extremely harsh prison sentences for content that they have posted online.[35]

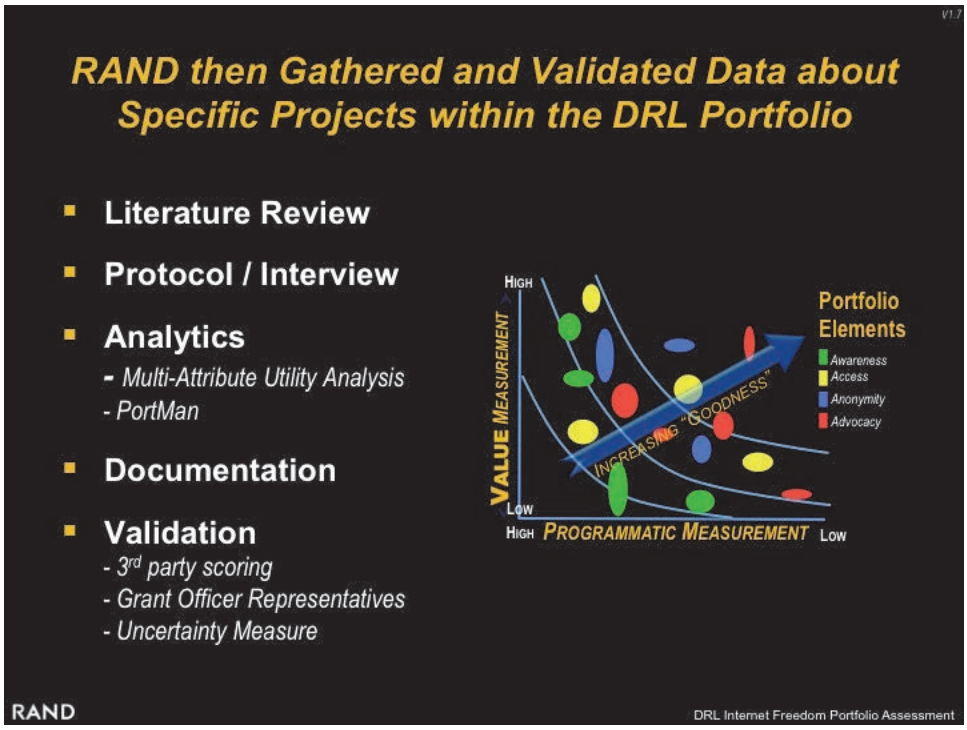
Similarly, there is a growing movement to shift from the current multi-stakeholder model of Internet governance to one that is controlled by nation-states. A growing number of states—led by China and Russia—are demanding that control over the Internet be transferred to a subcomponent on the United Nations, the International Telecommunications Union (ITU), which they can dominate.[36] To counter these moves, the United States can back campaigns that support sensible domestic and international regulations for the Internet and which preserve the multi-stakeholder model.

In short, access, anonymity, awareness, and advocacy are the four variables that the U.S. government can influence in order to increase the likelihood that an individual chooses to use the Internet to expand political space. This Internet freedom model forms the core of our analytical method and from this, we developed sub-attributes (see Figure 2) that could be measured and inputted into the PortMan methodology, which will be discussed in the next section.

Figure 2: Nested Measures Constitute Total Performance



[34] Open Net Initiative, *Profiles: China*, August 2012.
[35] Kelly, 2013, p. 10.
[36] Robert Faris and Rebekah Heacock, "Looking Ahead," in Gasser et al., 2013, pp. 86-87.



We employed the RAND Corporation's Portfolio Analysis and Management Method (PortMan) to evaluate DRL's Internet Freedom program portfolio.[37] RAND's PortMan method allows one to monitor performance and to make "data-driven decisions," which if used over time can assist in realizing the highest expected value from a portfolio.[38] The PortMan methodology also helps to ensure that a portfolio is appropriately balanced and that it aligns with the organization's overall objective.

To use the PortMan methodology, one must estimate the value and risk of each project based upon agreed upon set of metrics. The expected value of a project is a product of the expected value if a project is successfully implemented and the risk or likelihood of successful implementation.[39] We used the previously discussed Internet freedom model to develop metrics that were used to estimate the value and risk of each of the projects. Value, therefore, consisted of multiple components, specifically access, anonymity, awareness, and advocacy. Risk also included multiple factors, such as the feasibility of developing a new technology, and whether a project's product was likely to be embraced by the targeted community. In sum, we employed a multi-attribute utility analysis to compare the diverse projects included in DRL's Internet freedom portfolio. [40]

---

[37] For more on PortMan see: Richard Silberglitt, Lance Sherry, Carolyn Wong, Michael Tseng, Emile Ettedgui, Aaron Watts, and Geoffrey Stothard, *Portfolio Analysis and Management for Naval Research and Development*, Santa Monica, Calif.: RAND Corporation, MG-271-NAVY, 2004; Landree, et al., 2009.

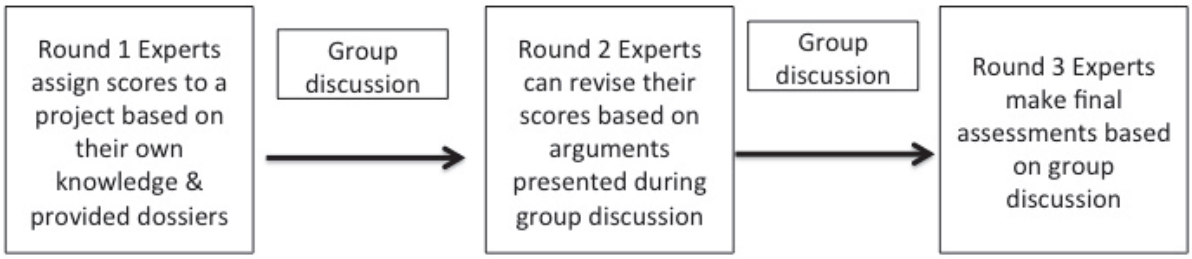
[38] Landree, et al., 2009, p. 5.

[39] Landree, et al., 2009, pp. 5-6.

[40] Lewis, et al., 1980.

To gather data on DRL's Internet freedom projects, RAND researchers conducted semi-structured interviews with each project team. Whenever practicable, the interviews were done in person. To ensure that the interviews were standardized and carried out in a replicable manner, we developed an extensive survey protocol, which was used in each of the interviews. The protocol included questions that would elicit information that could be used to estimate the expected value and risk for each project, including their background, desired outcomes, specific outputs, implementation strategy, methodology, project's alignment with key Internet freedom attributes, cross-project synergy, tool employment, measures of performance achievement and measures of effectiveness relevance, technical, programmatic, and acceptance risk.

Figure 3: Modified Delphi Method



We relied on a small group of subject matter experts (SMEs) and an approach that facilitates consensus building to estimate the value and risk metrics for each project.[41] The SMEs assessed each of the DRL Internet freedom projects on twenty-nine dimensions.[42] We used a number of our own experts in the modified Delphi consensus-building exercise to estimate the value and risk scores for each project.[43] To employ the Delphi method, we provided each SME with a dossier—a collection of standardized materials for each Internet freedom project, which were created from the data gathered during the interviews. In addition SMEs were provided with a scoring guide outlining all of the metrics and the range of scores. The Delphi consensus exercise typically consisted of three rounds, depending upon how far apart the SME's scores were. Each SME would score a project separately and then all of the SMEs would gather to discuss their assigned scores. In these discussions, particular attention was given to the rationale behind each

[41] For this project four RAND staffers who had expertise on Internet freedom and DRL's program served as SMEs. Silberglitt, et al., 2004; Landree, et al., 2009; Richard Silberglitt and Lance Sherry, *A Decision Framework for Prioritizing Industrial Materials and Research and Development,* Santa Monica, Calif.: RAND Corporation, MR-1558, 2002.

[42] The value score consisted of 17 different dimensions; the risk score was made up of 10 different dimensions; and the cost score included 2 dimensions.

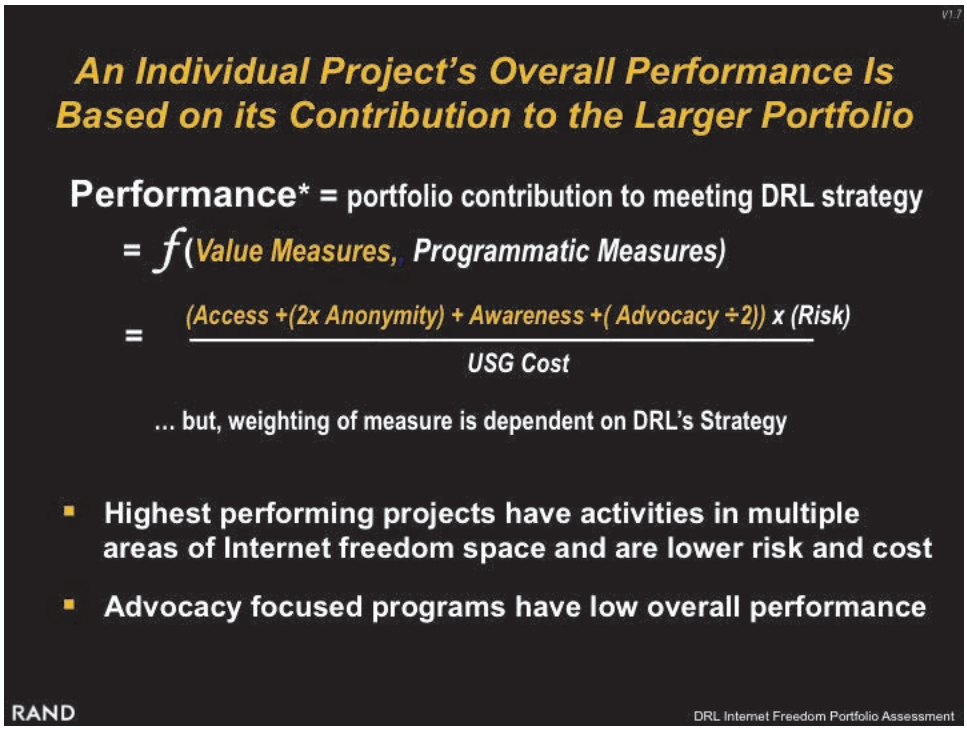
[43] Olaf Helmer-Hirschberg, *Systematic Use of Expert Opinions*, Santa Monica, Calif.: RAND Corporation, P-3721, 1967.

score as well as minority views. After the discussions, SMEs could individually change their scores based upon what they had heard in the discussions (See Figure 3). [44] Consensus was not necessarily reached on every metric, but this was reflected in the uncertainty assigned to each score. As a final check on outliers, we shared these scores with the DRL grant officer representative (GOR) assigned to the project to validate the findings from the Delphi method. In no instances did this result in modifications to the final scores.

The resulting data was further analyzed using a PortMan framework to determine the overall portfolio's performance and effectiveness. The PortMan analysis plots measures of value against measures of risk and cost. In the plot shown, a hypothetical program distribution is shown, with value measures increasing on the y-axis and programmatic measures of risk and cost decreasing along the x-axis. In this visualization, performance scores are largest in the top-right quadrant of the graph. Additionally, curved lines show the contours along which performance is equivalent (a project that is high-value and high-risk may have the same performance score as a project that is low-value and low-risk).

[44] This departed from the traditional Delphi method in that participants (in this case the SMEs) were not anonymous. The traditional Delphi method, however, does have drawbacks, which include the lack of live discussions and the fact that it is time consuming. For these reasons we used a modified Delphi method where participants knew each other's identities and participated in discussions, although they still independently made their assessments (i.e. scores). Silberglitt et al, 2004, p. 23. For a traditional Delphi method see Norman Crolee Dalkey, *The Delphi Method: An Experimental Study of Group Behavior*, Santa Monica, Calif.: RAND Corporation, RM-5888-PR, 1969.

Performance



Our Internet freedom portfolio assessment was based on the cumulative performance value of individual projects within the portfolio. The Internet freedom performance value of the individual projects was determined by each project's overall contributions to four major variables that impact Internet freedom and political space: 1) access to the Internet, 2) anonymity and security when accessing the Internet, 3) awareness and understanding of security threats and protective measures, and 4) advocacy for ensuring a free and open Internet compatible with the aforementioned U.S. policy toward free speech and human rights online.

A project's risk level and cost, both direct and indirect, to the U.S. government also influenced its portfolio contribution. Risk was assessed in three areas: 1) capability, or the reliability of a project's planned approach 2) acceptance, which assessed a project's credibility with users and deployment plan for the product, and 3) sustainability, which considered the project's planning for future activities and funding. Cost elements included a project's level of funding as well as potential indirect costs through management burden or international political exposure.

The major aspects of value, risk, and cost were each divided into a number of subcomponents developed in consultation with the RAND team, the State Department, and area experts. Each subcomponent was evaluated as a concrete metric with five levels of performance such that a project could be scored on a scale from one to five for each measure; in total, there were twenty-

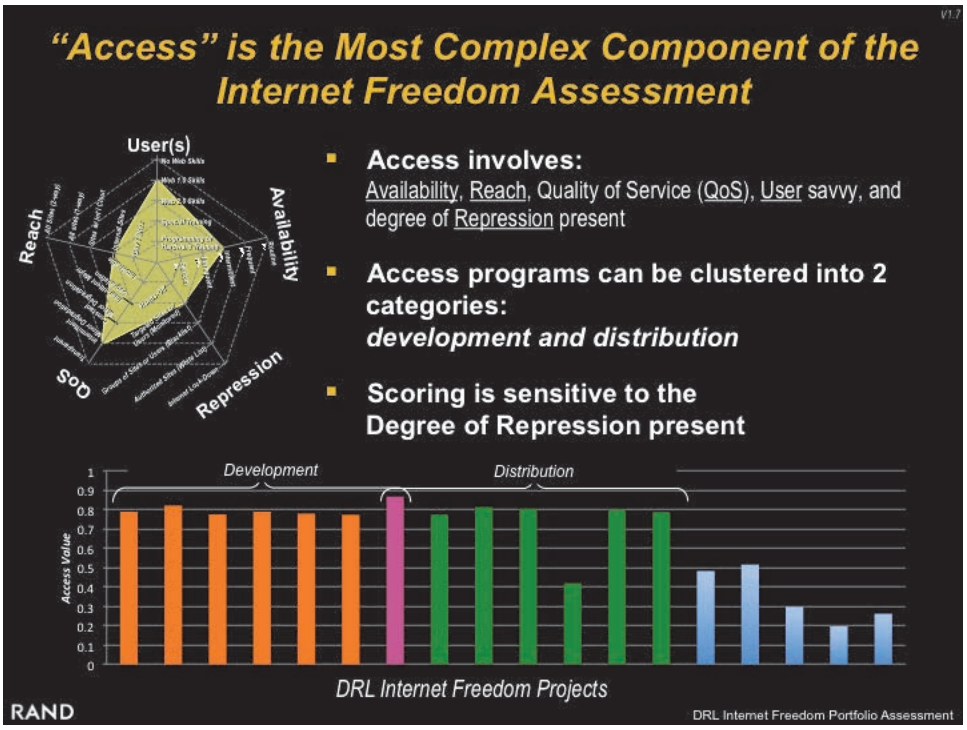
nine separate subcomponents that contributed to the performance calculation for each project. Following the data-gathering interviews and project dossier review, a panel of experts rated each project on all subcomponents. The subcomponent ratings were then aggregated to determine a project's contribution to a particular area.[45]

The major component scores (normalized to be out of one) in each area were then combined in accordance with the PortMan methodology to produce a single performance measure for each program. Under the PortMan framework, performance is a function of value added as well as programmatic measures, in this case risk and cost. The elements were combined according to the formula shown on the above slide. It is important to note that the four value measures, indicated in yellow on the slide, were not given equal weighting in the formula. Instead, they were weighted in accordance with the DRL program strategy, which emphasized anonymity when using the Internet as a key component, and viewed advocacy as a less essential aspect.[46] A useful feature of the PortMan methodology is that if the program strategy is altered, this weighting can be revised to generate new scores that measure project performance against the different strategy.

Unless otherwise indicated, the data shown in this document reflect performance scores based on the existing DRL strategy. Under this methodology, the highest performing projects were active in multiple areas of Internet freedom at comparatively low risk and cost. Additionally, because of the de-emphasis on advocacy, projects that focused primarily on advocacy efforts without incorporating other elements of Internet freedom received comparatively low performance scores. Conversely, projects that made a key contribution to anonymity on the Internet were among the higher performers.

[45] Aggregate score was calculated by taking the log of the relevant subcomponents and then normalizing the score. So for an element E with 3 subcomponent measures A, B, and C, the element score was E=log(A*B*C,5)/3.

[46] The DRL program strategy was communicated to the RAND team in a series of meetings, in which DRL proposed and approved the value weighting shown on slide 11.

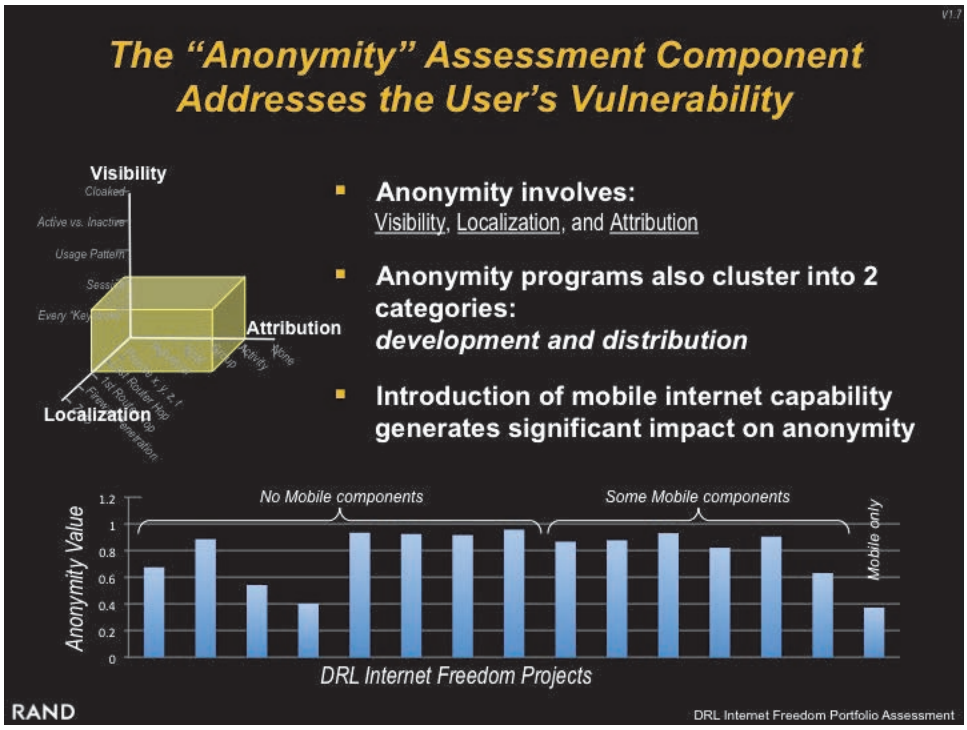


The access variable assessed a project's contribution to a user's ability to enjoy unfettered access to the Internet. Of the four value categories, this factor was the most complex, incorporating five separate subcomponents:

- User skill level: a measure of how technologically knowledgeable a user would need to be in order to maximize the project benefit
- Degree of repression: a static measure of the environment into which a product would be deployed with respect to Internet repression by the local regime. The repression scores for countries and regions were derived from the Freedom House 'Freedom on the Net 2013' publication.
- Reach: a measure of the degree of Internet access offered by a product in enabling a user to overcome censored or blocked sites
- Availability: the percentage of time a product was available and functioning as a circumvention tool, particularly with respect to whether there were any outages in service or if it would function in the event of a full Internet shutdown
- Quality of Service: a measure of the usability of a product under the intended conditions or environment into which it would deployed (in particular, whether use of the product would impact latency, error rate, etc.)

In general, projects that performed well in the access category were involved in either development or distribution of circumvention technology. Of the eighteen projects within the DRL programming, six were classified as development projects, meaning their primary activity was producing a new or improved circumvention tool. Another six projects were engaged in distributing tools and training Internet users in their usage.

An important aspect to note is that the access score was somewhat sensitive to the degree of repression in a project's intended deployment locale. Projects that targeted especially repressive countries or regions received a boost in their access score reflecting the value added of providing circumvention technology in areas where it was most needed.



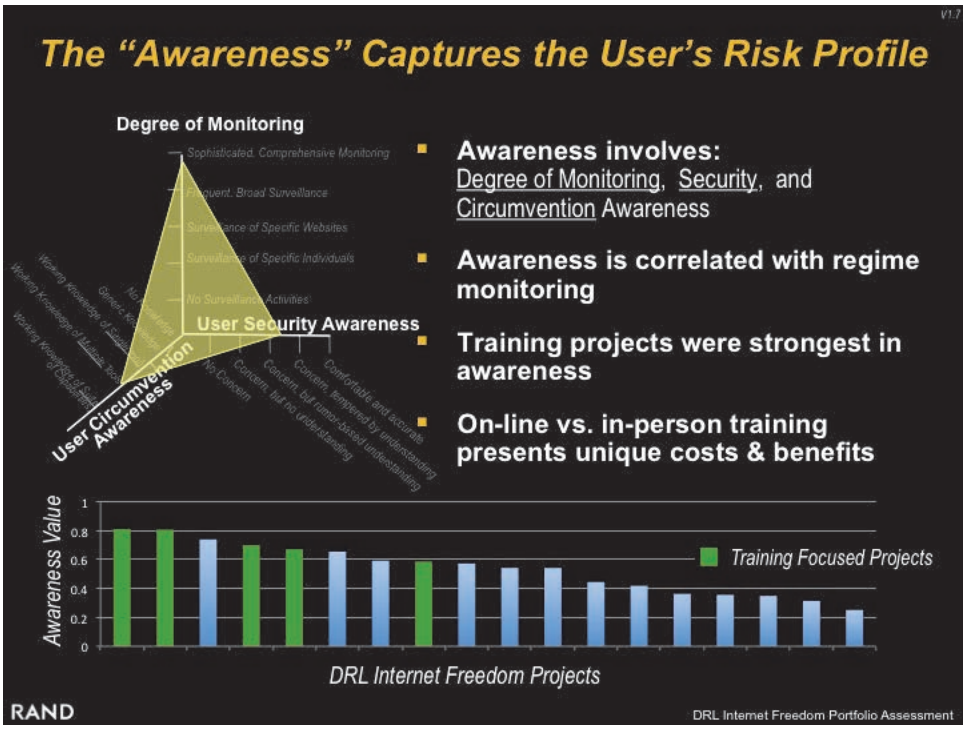
The anonymity variable assessed a project's contribution to a user's ability to securely and anonymously access Internet sites and send messages without regime visibility into the communications. Per the expressed DRL strategy, this factor was deemed the most important element of Internet freedom, as expressed by its double-weighting in the PortMan formula. The anonymity variable was divided into three distinct subcomponents:

- Visibility: a measure of the regime's ability to accurately detect and observe an Internet user's online activities when using the tools or techniques offered by the project
- Attribution: a measure of the regime's ability to connect online activity with an Internet user's real identity when using project offering
- Localization: a measure of the regime's ability to accurately identify an Internet user's geographical location

The majority of the projects active in the access category (producing or distributing circumvention technology) made similar contributions to anonymity, reflecting the growing recognition that unfettered access without security could be extremely dangerous for users.

However, the increasing use of mobile technology as the primary mode of Internet access worldwide posed particular challenges in the anonymity category. Projects providing user trainings and distributing tools acknowledged the problematic reality that while mobile technology is becoming more popular internationally, it is exceptionally vulnerable to regime monitoring with respect to localization and attribution. At present, there are no circumvention tools that guarantee anonymity when using mobile technology. The single mobile-focused

project in the DRL programming opted not to distribute mobile circumvention technology in order to avoid giving users a false sense of security.



The awareness variable was a measure of a project's contribution to a user's understanding of the sophistication of regime visibility into Internet usage as well as the measures that the individual user could take to increase his or her security. The three awareness subcomponents were the following:

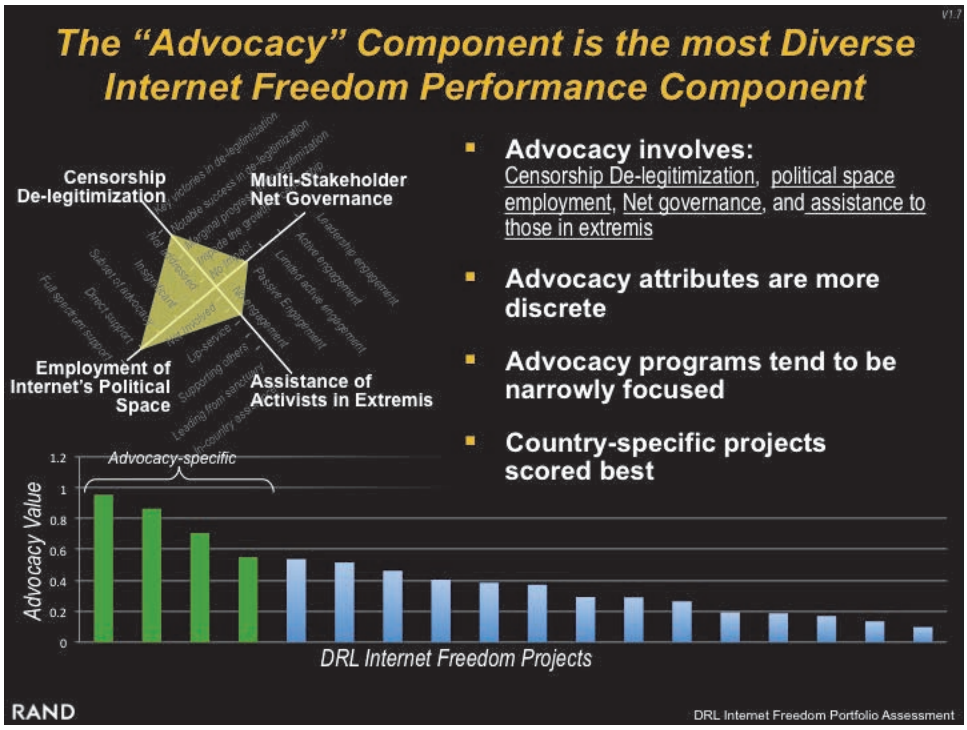
- Degree of monitoring: similar to the degree of repression measure in the access category, this metric evaluated the environment into which a product would be deployed with respect to Internet monitoring by the regime. As with repression, the degree of monitoring scores for countries and regions were derived from the Freedom House 'Freedom on the Net 2013' publication.
- User security awareness: a measure of the project's impact on the intended user's understanding of their vulnerability to regime monitoring
- User circumvention awareness: a measure of the project's impact on the intended user's knowledge of the circumvention technology available to them and its appropriate usage

Scores for user security and circumvention awareness were tabulated with a slightly different procedure. Because the emphasis for these measures was on project *impact* on user awareness, the measures were estimated for users before the project was implemented as well as after. The project score was then measured by the difference, or increase in knowledge pre- and post-project.

As with access, the inclusion of the static degree of monitoring measure meant that the geographic targeting of projects had an impact on their scores in this category. Projects that directed their efforts at countries with more repressive regimes received a scoring benefit that

reflected to the increased importance of user security awareness in these areas. Additionally, because of the way the impact criteria were scored here, projects whose intended users had a low understanding of regime monitoring prior to their interaction with the project had more potential for impact than projects that targeted highly knowledgeable users.

The highest performing projects in this area tended to be training-focused, or incorporated training as a major element of their project activities. We found that there was a high degree of diversity in the strategies projects employed to train users, ranging from short, mobile "micro-sessions" in Internet safety to detailed, month-long courses. In addition, some project trainings were implemented on an in-person basis, which often meant individuals had to leave the country to attend trainings in a less repressive region; other projects opted to place all training materials online and teach courses in a virtual classroom. Both strategies have merits and drawbacks but may be tailored to the unique challenges faced in different regions.

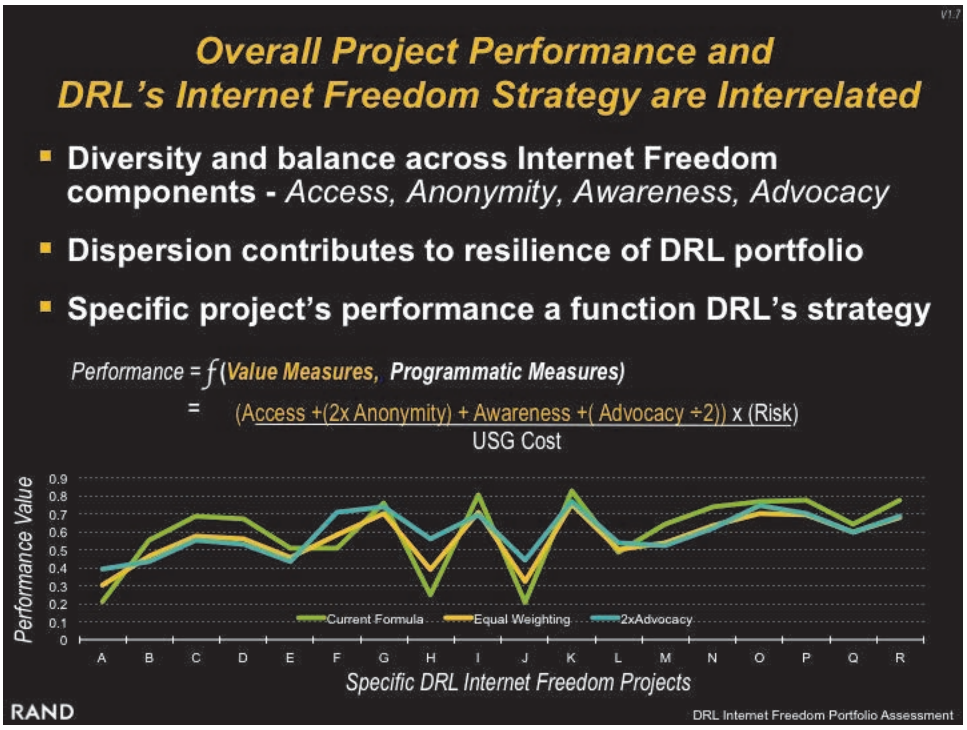


Advocacy was the final variable included in the measure of project value, and referred generally to project efforts that influenced environmental factors with respect to the Internet or promoted the concept of a free and open Internet compatible with U.S. policy toward free speech and human rights online. The four subcomponents contributing to the advocacy measure were less interdependent; in other words, a program did not need to perform well in all four categories to contribute value. The four subcomponents, developed in discussion with DRL and based on their objectives, included the following:

- Censorship de-legitimization: efforts to make political censorship an unacceptable activity
- Multi-stakeholder net governance: efforts to make net governance more inclusive of civil society participants
- Assistance to activists in extremis: provision of emergency or legal services to activists persecuted or prosecuted by a regime in regards to online activity
- Employment of Internet's political space: assistance and training of activists on effective techniques for using the Internet to expand political space

We observed that projects with a focus in one or more of the other value categories made only small, second-order contributions to advocacy. The four advocacy-specific projects in the DRL portfolio tended to be narrowly scoped and made fewer contributions in the other value categories, suggesting there is less interaction between this element and the other three categories, at least in practice. Because of the reduced weighting for advocacy in DRL's PortMan strategy, these projects tended to receive lower-than-average total performance scores, although the projects themselves seemed topical and well run. Finally, while some of the

advocacy projects were active in multiple countries and regions, we observed that some of the strongest projects took a more focused approach, specializing in a single country and employing a multi-pronged effort to address issues of advocacy from several directions.



Assessing the individual Internet freedom factors within the portfolio—the access, anonymity, awareness, and advocacy contributions just discussed above, provides one perspective of the portfolio's value. We were also interested in assessing the alignment between DRL's Internet freedom strategy and the performance of its funded portfolio of projects. This alignment was captured by looking at the cumulative aspects of these the four factors as well as risk and cost, as discussed earlier. DRL was interested in both balancing the contribution from all four factors, but was also aware of the critical need for protecting at-risk users within authoritarian regimes.

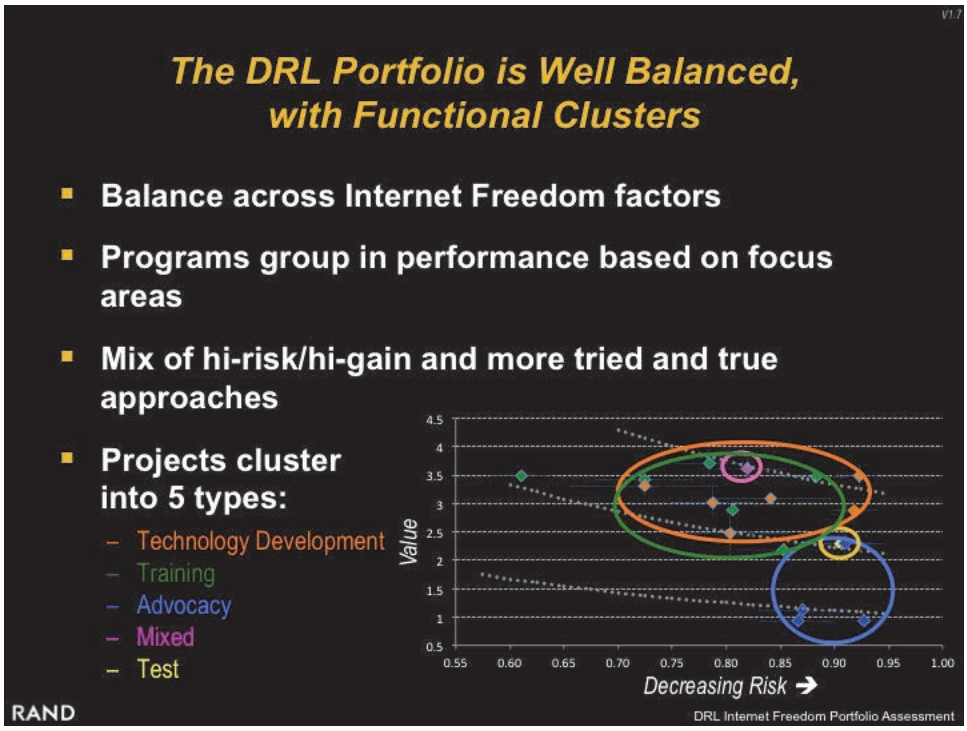
Strategies should change over time in response to evolving circumstances. This has proven to be true with the DRL Internet freedom portfolio. Initially, DRL focused on improving access to the Internet in repressive states by funding circumvention tools, such as virtual private networks (VPNs) and proxy routers. By the time that we began our assessment, DRL had determined that access by itself was insufficient for realizing the goal of expanded political space. Additionally, users needed their access to be anonymous and their communications to be secure. Consequently, DRL instructed us to double the value of anonymity in our performance equation.[47] Around the same time, DRL decided that advocacy was less of a priority than the other variables, so its value was halved.[48] As shown in the graphic above, the relative weighting of Internet freedom factors, as they reflect the DRL strategy, can normally have a 10 -20% impact on a projects score. As an excursion, we varied the relative weighting of the advocacy

[47] Meeting with DRL Internet freedom team, 10 Jan 12, Department of State, Washington DC.
[48] Meeting with DRL Internet freedom team, 14 Nov 11, Department of State, Washington DC.

variable, from that of the current DRL strategy, to that of equal value with the others, and to one twice the value of the other factors. Such variations had a notable, but contained, impact except when projects were very narrowly focused (e.g. projects "H" and "J"), and in these cases the impact exceeded 100%.

DRL's Internet freedom strategy is likely to change again. Increasingly, there is a recognition that there is not a technical solution that can ensure a free and open Internet. Instead the future of the Internet is also impacted by legislatures, judges, and international organizations. Consequently, one would expect that advocacy may become a more important part of DRL's Internet freedom strategy. That is not to suggest that previous strategies were flawed; rather, they may have been appropriate for their time, but circumstances have since changed. One of the key benefits of our assessment methodology is that it can adapt to different strategies. If it is employed over time, it can help to ensure that DRL's strategy remains aligned with its funding decisions.

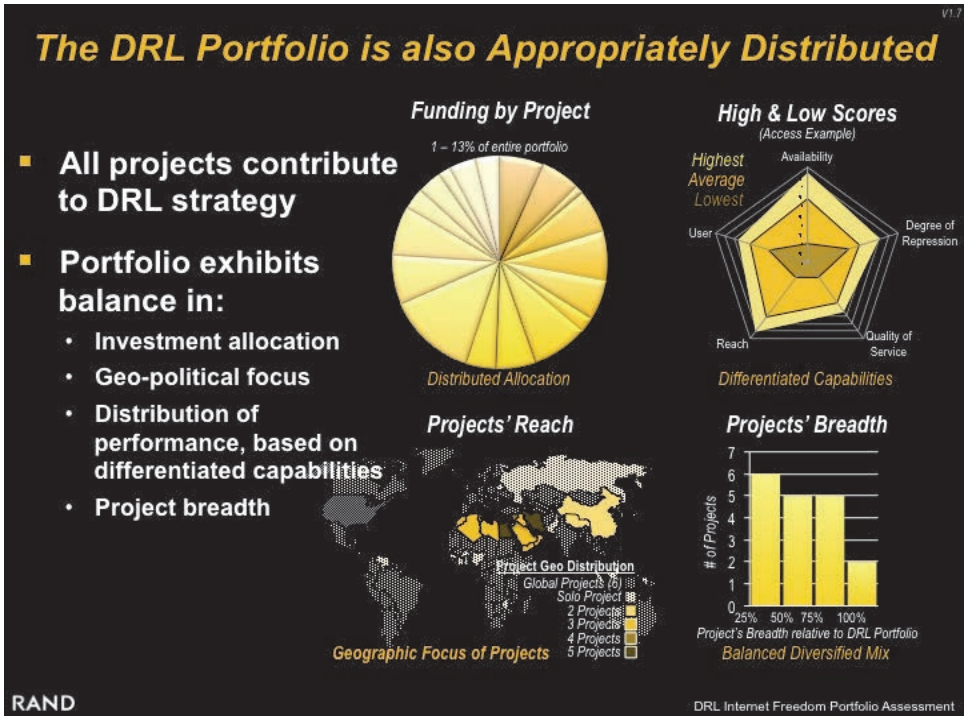
Balance and Diversity



In a broad sense, our assessment of the overall portfolio found a strong diversity of effort and balance across the four variables that impact Internet freedom and political space (access, anonymity, awareness, and advocacy). We found these factors were distributed across projects roughly proportionately to their weight in the portfolio performance calculation. Each was addressed by more than half of the projects, which added robustness to the portfolio. We also found, that while the projects exhibited diversity in their scope, objective, and approach, they were generally balanced in their contribution to both overall performance and the four functional variables that were specifically measured. (The two outliers were projects narrowly focused on sub-components of advocacy). We also determined that the portfolio contained a mix of both high-risk/high-gain and tried-and-true approaches. While a handful of projects employed very similar objectives or approaches, these appeared appropriate to the scope of those projects and desirability to have redundancy in that segment of the portfolio. We also found that the diversity along numerous portfolio dimensions was desirable from a portfolio risk-reduction perspective. The portfolio, while balanced, diversified, and distributed among eighteen projects, maintained a coherency with DRL's strategy and a collective unity-of-effort to be of continued value to both targeted users and diplomatic American interests.

Due to this balance and dispersion of Internet freedom factors among DRL projects, we found it helpful employ an analytic filter to differentiate the projects. After testing several

constructs, we found it most helpful and natural to group projects based on their objectives. This provided five generic categories for parsing the projects those with a technology development objective, a training objective, an advocacy objective, one mixed program, and another that provided testing resources for technologies developed by other projects. After categorizing each project by its goal and plotting its performance, we found that projects with the same objective tended to score similarly and cluster together. The technology development and training clusters contributed most to the portfolio's value, while advocacy projects contributed the least, which reflects advocacy's lower weighting in the performance equation. More interestingly, within each of the three major project clusters there was of balance high-risk approaches which hold out the promise of significant gains, along with more traditional and proven approaches, which had a higher probability of success but also promised lower returns.

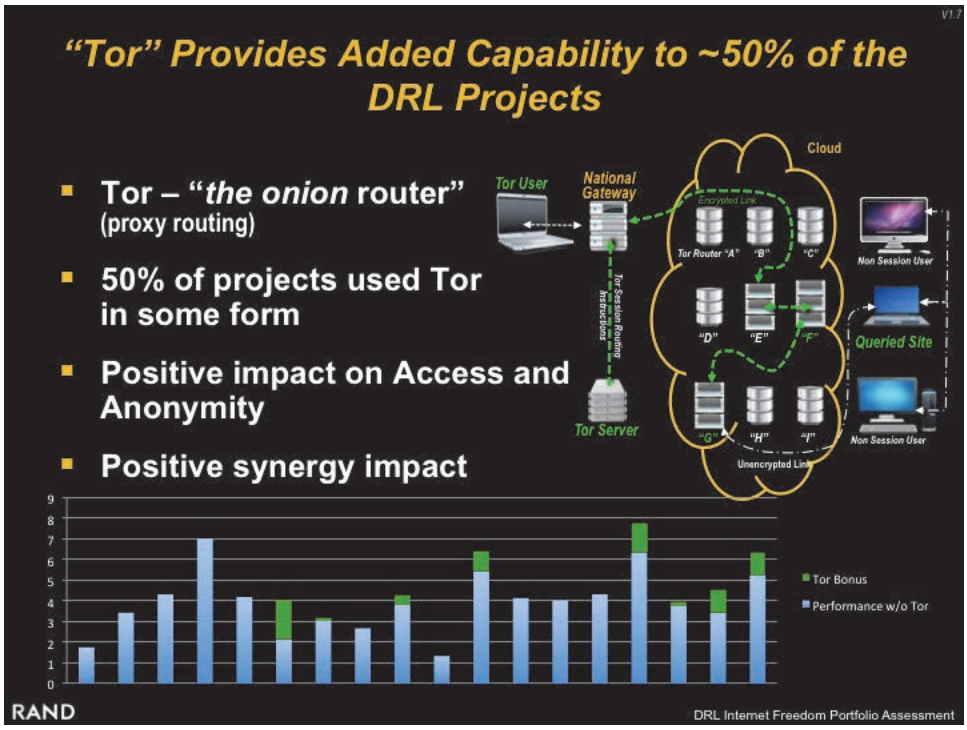


Beyond balance in objectives, approaches, and Internet freedom factors, the portfolio exhibited other characteristics of balance, such as attributes of the individual projects. Again, the assessment revealed the DRL Portfolio as balanced; yet diversified, with respect to project investment allocation, geo-political focus, breadth, and distribution of performance (based on differentiated capabilities). While all the funded projects were clearly aligned with Internet freedom objectives, they provided a multiplicity of means in seeking to meet those objectives.

The investment allocations were fairly evenly apportioned to projects of differing size, ranging from 1% to 13% of the portfolio's total value. The geographical reach and geo-political focus of the projects spanned from global to single country, with an emphasis on regions and countries of particular interest to the United States government (e.g. Iran, Middle East and North Africa, and China). Five of the projects were targeted at global Internet users, five had single country focus, and eight had a regional focus.

One aspect of the effectiveness of the assessment process was the degree to which it captured, in a quantitative manner, the qualitative differences between projects. The methodology we employed assessed a large number of qualitative project characteristics and then assigned a quantitative grade to them, based on expert elicitation and judgment derived from the modified Delphi approach. The spider graph above illustrates the distribution of the quantitative grades within the portfolio for one of the Internet freedom factors (access). The distribution of performance scores shown are indicative of the methodology's ability to differentiate performance among projects and is in agreement with qualitative observations. It also underlines the larger portfolio balance, since with different projects having different objectives and approaches, their detailed performance scoring would also be expected to vary.

Finally, the breath of individual projects within the portfolio was also diverse. While six projects were principally focused on a single Internet freedom factor (access, anonymity, awareness, or advocacy), five spread their focus between two of the factors, another five applied their efforts to three of the factors, and two addressed all four with a roughly equal level of effort. This is reflective of the diversity of project approaches and the effective distribution of portfolio resources across DRL's Internet freedom agenda.

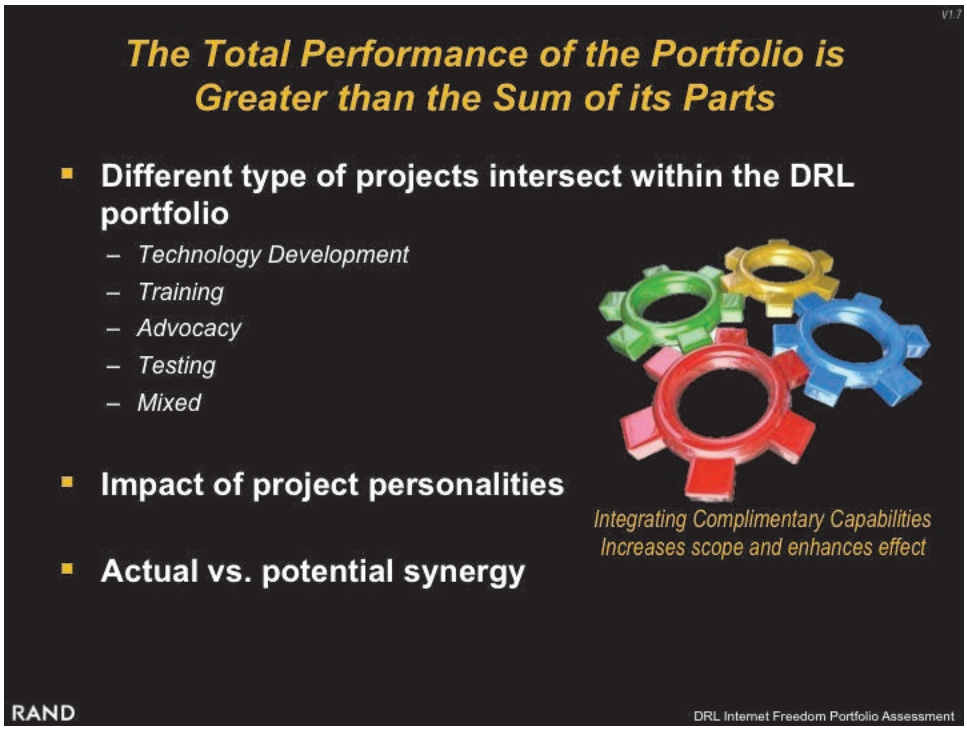


Despite the diversity and balance within DRL's portfolio, we noted one commonality among many of the projects: many relied upon a specific circumvention tool—The Onion Router (known as Tor). Tor is a multiple-hop proxy router that works by routing Internet traffic through several proxies thereby bypassing firewalls and protecting the user's identity. The cartoon above depicts how Tor operates. While Tor does receive USG funds, it is not a direct DRL grantee, and, therefore, was not directly assessed as a project within the portfolio.[49] But because half DRL's projects used Tor to varying degrees, its impact on the portfolio was of interest.[50] We found that Tor had a positive, but not determinate effect on those projects which included it in their approach. The degree of impact was a function of the project's reliance on Tor for circumvention capability, which influenced a project's access and anonymity performance scores. An additional unexpected benefit from Tor was the positive contribution it made portfolio's synergy, which will be discussed further in the next section.

[49] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Deploying Low-Latency Anonymity: Design Challenges and Social Factors," *Security & Privacy, IEEE ,* Vol.5, No.5, September/October 2007.

[50] Five of the projects had individuals affiliated with Tor as members of their technology development teams.

Synergy

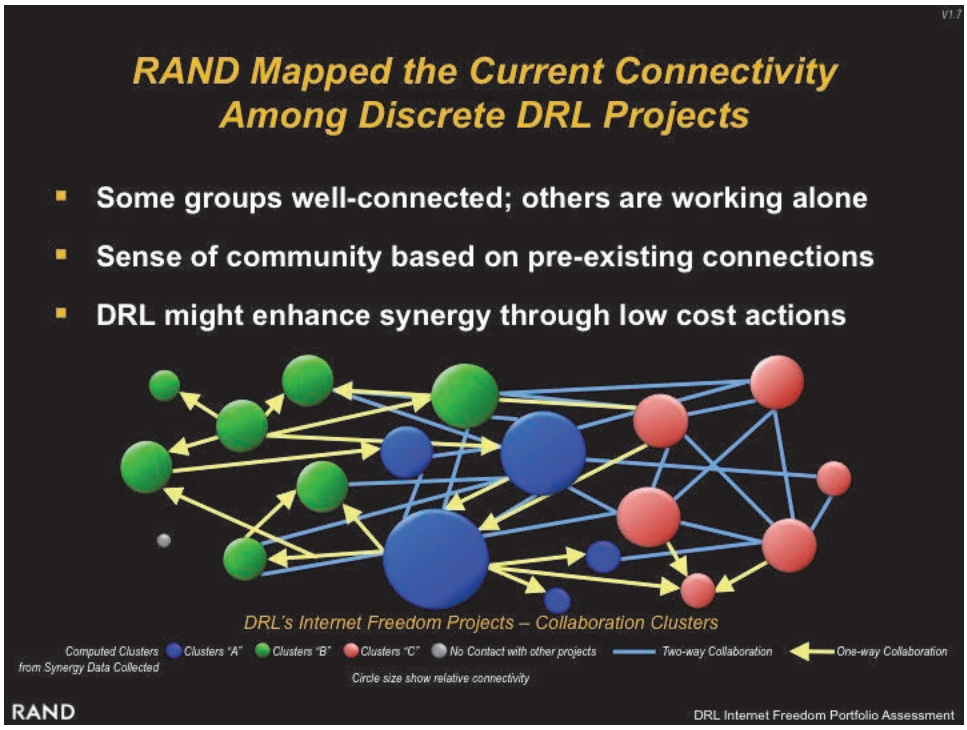


A key observation of the portfolio assessment was that the total impact of the program is greatly enhanced by the interaction and collaboration between implementers. Projects from the five above cluster areas intersect within the portfolio and produce opportunities for project synergy that can lead to enhanced project, as well as portfolio, performance. Such linkages could also provide conduits for additional collaboration beyond the scope and timeframe of the DRL grant. The potential benefit of this synergy is substantial. For example, projects engaging in technology development could greatly benefit from interaction with groups testing for security flaws; training programs could distribute newly developed circumvention tools and tailor them for a particular setting, etc. Nurturing and enhancing this synergy would provide DRL with the opportunity to notably leverage both the effectiveness and impact of its Internet freedom investment, while reducing portfolio risk.

While we did not develop a formal methodology to assess the synergy within the DRL portfolio, the interviews provided insight into where opportunities exist for enhancing synergy. One standout observation was that from an individual project perspective, generating synergy was often challenging because many projects did not approach their work with a collaborative mindset. There was also a tension due to the competition between projects for scarce resources.

As a result, we found that there was a notable difference between the actual synergy effects and its potential for creating a stronger portfolio.[51]

[51] These observations were debriefed to the DRL portfolio management team during the course of the RAND assessment. By the conclusion of the assessment several informal RAND recommendations regarding portfolio synergy had been adopted.

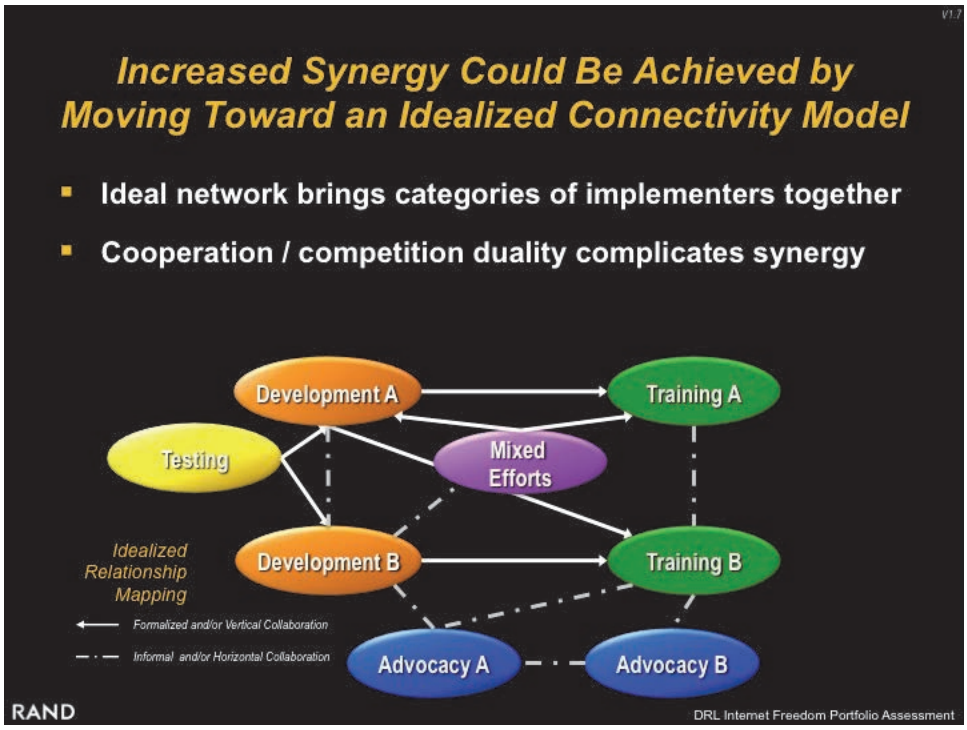


To better understand the portfolio's potential synergy RAND researchers mapped the existing connections between projects, which resulted in the network depicted above. Some implementers had strong, established connections with other groups (shown above as large circles), but these were often based on pre-existing connections and relationships. Nevertheless, these ties were beneficial as projects shared best practices and technologies, and helped each other to overcome problems. Others had fewer ties to other groups (shown as proportionately small circles) and one group was isolated with no connections to other DRL grantees (shown as a disconnected grey dot). Some connections were one-way (shown above in yellow), while some were more equitable or two-way (shown in blue). As previously discussed, Tor produced an added element of synergy by providing capabilities to a number of projects. When we applied a commercial network analysis tool to our recorded observations it produced the above characterization of the portfolio.[52] This process revealed that there were three principal clusters of collaboration within the portfolio, which is similar to what we informally observed. Interviews with project leaders suggested that these clusters were mainly the result of previous working relationships between persons from different projects that carried over to DRL portfolio.

While there is considerable value to the existing ad hoc connections, we determined that more networking would help to realize the portfolio's full potential. Additionally, we believe that DRL could do more to encourage informal cooperation as well as more formal partnerships. DRL heeded our advice and has taken a number of steps to encourage collaboration between its grantees, by setting up mechanisms to facilitate communication and holding gatherings so that

[52] We used Gephi, an open source interactive and visualization software for network analysis.

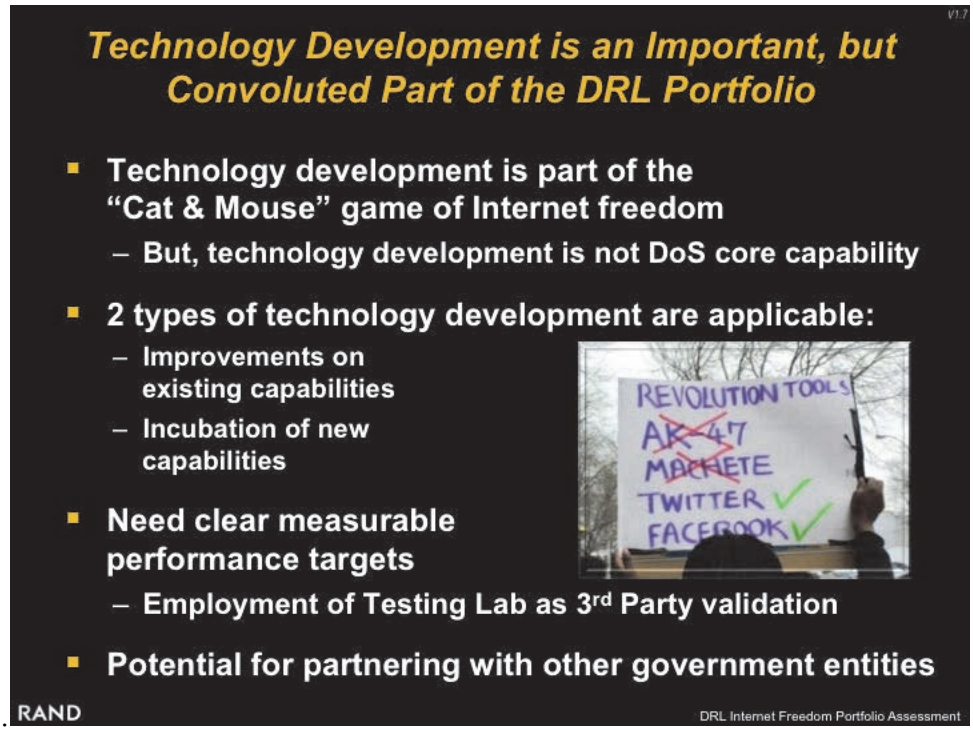
grantees can meet and interact with each other in person. DRL convenes an annual implementers meeting which is useful for making introductions, learning about other projects, and building trust. Additionally, DRL encouraged the implementers to create a listserv so that they could directly reach out to each other. These are important steps that have been beneficial, but we believe that DRL should do more.



Based on our understanding of the DRL portfolio and its objectives, we constructed an idealized characterization of the portfolio's potential synergy shown above. The five generic categories discussed earlier (technology development, training, advocacy, testing, and mixed efforts) served as the synergy building blocks. In attempting to maximize the portfolio's synergy, there would be an inherent tension between projects cooperating and competing in DRL's limited resource environment. Therefore, collaboration within clusters (i.e. projects that have similar goals), where competition might be highest, would need to be incentivized by DRL. Internal cluster cooperation would involve sharing best practices and lessons learned. Similarly, there is potentially great value to cooperation between clusters (i.e. projects that are pursuing different objectives) because there is a natural division of labor. Nevertheless, DRL may need to broker between cluster cooperation, which often does not materialize because it goes beyond the scope of the grant. For example, technology developers need agents to distribute their tools and trainers need Internet freedom tools to protect and empower their students; therefore, DRL could benefit both the portfolio and the individual projects by facilitating their partnering.

Because the potential for cooperation was not fully realized, we argue that synergy is one area that could be improved in notable ways. Synergy presents an especially worthwhile investment because of its low cost and high potential payoff. More than just increasing the portfolio's effectiveness and efficiency, enhanced synergy could provide other positive latent effects. Even if projects do not immediately collaborate from start to finish, the latent relationships facilitated by their interacting with other DRL participants may bear fruit at a later time. In particular, fostering personal and organizational ties, along with enhancing, trust would

position the Internet freedom community to organically and rapidly respond to rapidly developing Internet freedom-associated future crises.

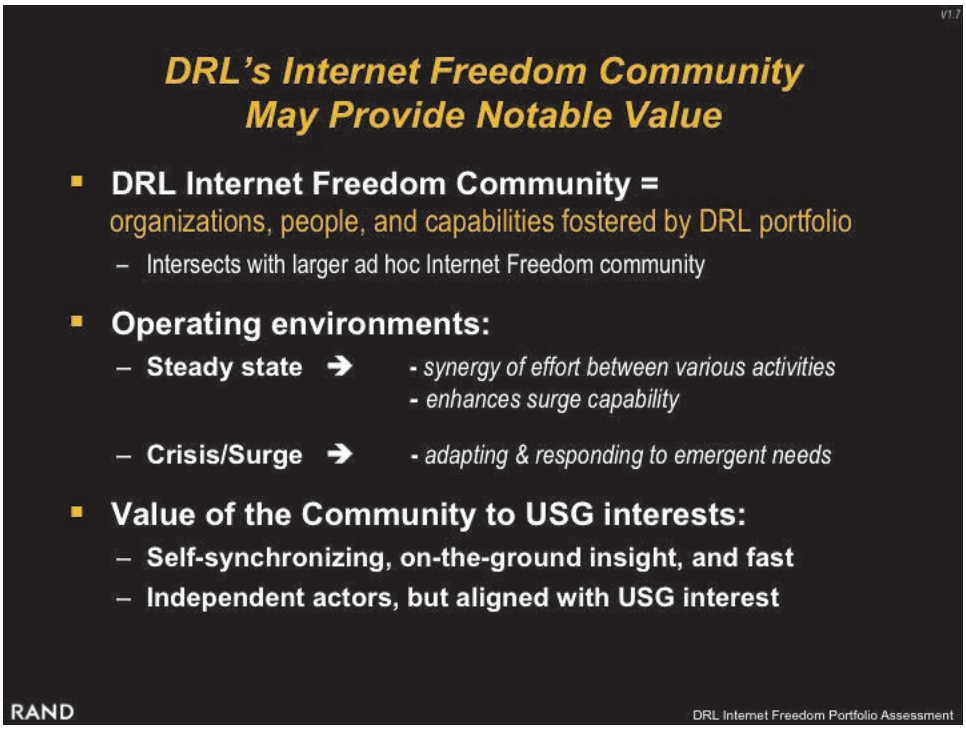


Developing new technologies that enable individuals to have unfettered and secure access to the Internet is a significant, but complicated part of the DRL portfolio. The struggle between those promoting Internet freedom and those trying to control and censor the Internet is a fast-paced cat and mouse game. Consequently, the speed of this contest often outstrips the grant cycle, and implementers often have to modify their proposed deliverables in response to developments on the ground. Responding effectively to the countermoves made by authoritarian governments is difficult under any circumstances. This predicament is further complicated by the fact that technology development is not a traditional State Department activity and, therefore, not one of its core capabilities. Partnering with other U.S. government entities who have proven technology development infrastructure and core competencies could potentially help to overcome this limitation.[53]

[53] The Defense Advanced Research Projects Agency (DARPA), who also has a Internet freedom technology development program, participates in the selection of DRL projects to be included in the portfolio. Based on interviews with the DARPA and DRL Program Managers, we found that there is an informal understanding between DARPA and DRL that DARPA will tackle longer-term and technology hard challenges, and DRL would focus their portfolio on nearer-term challenges. Since at the time of this assessment there was little commercial market demand for increased security for non-institutional users in their everyday communications, there was a paucity of for-profit firms with which DRL to work

At the broadest level, the State Department is interested in nurturing two types of technological advancements: evolutionary improvements to existing circumvention and anonymity tools and the incubation of new revolutionary Internet freedom capabilities. DRL's current portfolio has a mix between improving or tailoring to particular countries known and proven tools and supporting the development of new and paradigm-shifting capabilities.[54] Doing so effectively, however, requires clear measurable performance targets for the grantees and the use of trusted third parties (e.g. an independent lab) to test and validate both types of tools.

[54] Based on the above DRL-DARPA understanding, the technology development aspects of DRL's strategy was to support low-risk country-targeted, global, an uniquely innovative technologies that were not being adequately addressed elsewhere in government or industry.

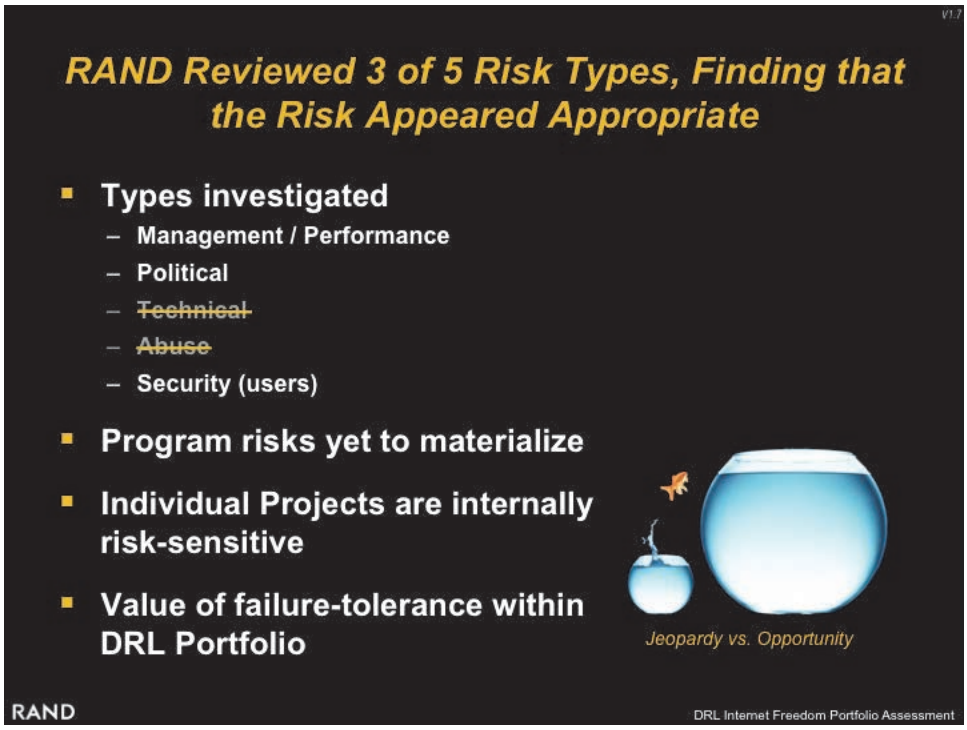


DRL's investment in Internet freedom should have enduring value that extends well beyond the life of the individual grants. In particular, one of the most important effects of the DRL portfolio appears to be the community it nurtures. Although more might be done, DRL has taken steps to maximize the return on its Internet freedom portfolio by bringing together the individuals, organizations, and tools it supports. The DRL Internet freedom community is only one sub-set of the larger Internet freedom community, which includes organizations supported by other U.S. agencies (including DARPA, USAID, the BBG, and perhaps other unacknowledged organizations), foreign governments, non-governmental organizations, and private citizens and corporations, such as Google.[55]

The DRL Internet freedom community could play different roles, depending on the situation. During normal times, the DRL Internet freedom community is focused on increasing the State Department's steady-state capability to promote freedom online. As discussed above, it does so by encouraging formal and informal collaboration between grantees to improve the efficacy of both projects. At the same time, fostering these ties also develops latent surge capacity to respond during Internet freedom-associated crises. At critical moments, the DRL-sponsored community has the capacity to rapidly and independently respond to developments in an effort to expand political space. In these circumstances, a self-synchronizing community comprised of independent actors whose interests are aligned with the United States government

[55] For more on U.S. government agencies involved in Internet freedom see: Figliola, 2011; and Patrcia Moloney Figliola, *Promoting Global Internet Freedom: Policy and Technology, Washington, DC: Congressional Research Service, May 26, 2011;* Google, *Google Take Action*.

is not only well-positioned to react, given its grassroots connections, but it also is more agile and capable of responding in a timely fashion than the government. Moreover, by having the U.S. Government stay in the background, it reduces the potential for blowback. In short, a key lasting value of the DRL portfolio is the relationships it builds and the capability of those relationships to generate a rapid coherent response to emergent Internet freedom crisis.



Besides assessing the DRL portfolio's performance, balance, and alignment with strategy, RAND also assessed potential portfolio risk. We defined risk as exposure to the chance of future negative events. To better dissect the portfolios risk we parsed it into the five different, mutually exclusive, components shown above. We then assessed individual projects against these risks to assess their impact on the cumulative portfolio risk.[56] Management/performance risk addressed with the projects' ability to effectively and efficiently deliver on their stated objectives. The management aspect was captured through a checklist the background and experience of the project's managers, the staff's functional expertise, internal management practices and controls, and its operating measures of effectiveness and performance. The performance aspect was assessed for its alignment and contribution to DRL Internet freedom strategy. Political risk captured a project's potential to cause negative diplomatic, congressional, or media effects.[57] Political risk assessed the project's targeted field on operation, the degree of real and potential interest of the host government in its operating domain, the project's public profile and ethical standards, the parent organization's attitude toward working with the media and its relationships with various government entities, among other factors. Technical risk dealt with the project's potential to fall short of its stated capability thresholds. Abuse risk addressed the potential for

[56] At the time of this assessment different projects were in different stages of execution. Investigation of risk was based on material available at the time and the competency and track record of project staff to successfully execute their objectives. In agreement with DRL, is was understood that this assessment could only reasonably investigate near-term risk, and that mid- and far-term risk were out of the assessment's scope.

third parties to use the project, or its products, for illicit or undesirable purposes. Security risked looks at the exposure of a project's intended users to regime retribution for their use of a project's products or services. Security risk assessed the project's security protocols for protecting staff and users, its history in working in similar environments, and its compliance with USG regulations and standards.

During this particular assessment, RAND assessed each project with respect to only management/performance, political, and security risk. Technical and abuse risk were beyond the scope of the current assessment.[58]

Across the DRL suite of projects we found the assessed risks had yet to materialize.[59]That does not mean that problems might not arise in the future. In working with the various projects, RAND found each to be sensitive to those three risks -- most especially security risk. Beyond complying with USG guidance, project personnel appeared to feel a deep-seated personal responsibility to take security for their users to a higher level.

Portfolio diversity was also evident in the area of management/program risk, where some projects had more exposure than others due to the ambitiousness of the project's objectives. We viewed this as risk-tolerant approach as both acceptable. If DRL chose to drive-down this risk they would also need to drive -down project objectives, which would notably drive-up overall portfolio risk—with the potential to undershoot the portfolio's potential value to users, the Internet freedom community, and U.S. interests. As illustrated in the cartoon above, we found that DRL needed to balance its portfolio between jeopardy vs. opportunity. Raising the acceptable risk threshold to high could forfeit significant accomplishments. We assessed DRL as having found an appropriate risk balance.

[58] Subsequent to the assessment covered by this report DRL engaged RAND to assess technical and abuse risk, which will the subject of a forthcoming report.

[59] The majority of projects were evaluated in their early stages, and therefor in those case management/program risk was projected for their assessments.

We identified five key characteristics for a well-run project—which correspondingly has a strong correlation to successfully managing portfolio risk. The first three of these aspects are dependent on the project's human capital – first, the person(s) who conceptualized the project and/or continued to serve as its champion within the project's larger host organization; second, the team member(s) with the functional expertise that ensured the project had a sound technical or methodological approach, and: third, the project manager(s) who ensured there is a viable roadmap for achieving the project's objective and being on-cost and on-schedule in its execution. In the strongest projects, three different individuals separately handled these three areas, though there were notable exceptions when one individual simultaneously and successfully filled two roles. When one individual attempted to fill all three roles, some aspect of the project appeared to suffer from inattention.

A fourth aspect of well-run projects we observed were its linkages to other projects, pockets of expertise, and insight outside of the particular project. Those projects that interacted with knowledgeable external actors appeared to use the insights gained to fine tune their approach and help them navigate roadblocks encountered during execution. Those projects that specifically interacted with others in the DRL portfolio also appeared more comfortable in their DRL working relationship and knowledgeable.

The final aspect, the program environment, addressed the circumstances in which the project was executed. The more benign the program environment, the lower the stress on the project, and the higher the probability of achieving its objectives. The program environment had three elements, the project's host organization, the project's working relationship with DRL, and where the project was being executed. We found that projects had a spectrum of host

organizations, from large universities, large, medium, and small non-profits, down to basically single person operations. We observed no correlation between the nature of the host organization and the performance of projects. This is likely a result of DRL's grant screening process, which filters for quality. From the project's perspective, we observed a consistently positive working relationship with DRL across the portfolio.[60] Finally, there was a large diversity in where projects were being executed, from the most authoritarian of states with high personal risk to participants, to locations with only rudimentary IT infrastructure, to high tech test environments. We again viewed this portfolio diversity as an indication of its robustness.

The specific criticality of factors learned above: first - the distribution of leadership workload among the champion, the functional expert, and project management; and second - the desirability of strong external links, were not part of our formal assessment. They were observed and learned during the course of the assessment, and therefore were not part of the assessment's formal methodology. Nonetheless, we found a strong informal correlation between their presence and low management/performance risk. They also correlated with projects staffed by more experienced personnel.

[60] These observations were made in the early phases of each project. RAND has no data on the working relationship beyond that observation period. Those organizations who had worked with DRL previously through a project's full life cycle indicated that, based on past experience, they expected no changes in the DRL working relationship.

While we assessed numerous strong points in the DRL Internet freedom portfolio, there were some underlying areas of potential concern, but many of these are outside of DRL's control.[61] The most prevalent and acute problem is one of staffing. Across the portfolio, projects' top tier concern was access to high quality IT talent. As mentioned earlier, Internet freedom is playing a cat & mouse game between those who seek provide all the benefits of the Internet to all the world's citizens and regimes who seek to repress the Internet to enhance their regime's stability. These authoritarian regimes apply their best available IT talent to enhancing their own security by repressing their citizens Internet activities in one form or another. On the Internet freedom side, this work is principally done by non-profits and NGOs. In order to effectively challenge repressive regimes, NGOs need highly talented IT professionals. But NGOs cannot effectively compete for these individuals in the commercial marketplace, where employment choice is primarily a matter of monetary compensation. Rather, NGOs are limited to a very small subset of the larger market, that part composed of IT experts who are motivated more by mission than money. While there are some truly inspiring IT experts within that small subset, the number of such experts is insufficient to meet the demand.

Another concern is that some projects are narrowly focused in scope and hold little promise of successfully being scaled up. At times, it seems as if this constrained focus was not an issue of resources alone, but rather due to the approach that the project had taken. As will be discussed later, at times a small group of opinion leaders may have a disproportionate impact on political

[61] These concerns were those noted as of April 2013, subsequent international events and USG actions may have impacted their significance.

space; and therefore, it may be wise to target this select group. Nevertheless, this is not always the case and when possible, it is often valuable to expand pilot projects.

Of lesser, but still notable, concern, are three other matters. First, since Internet freedom is a relatively new field for both liberal democratic governments and NGOs, some organizations are starting from scratch, while others have only a few years of Internet freedom project experience. Until a body of best practices and lessons learned are codified and accessible to implementers, many will find themselves expending effort on problems previously solved by others. Second, many of the projects would like to better support the multi-stakeholder approach to Internet governance, but are not certain how to do so given the many different actors and institutions involved. And third, the nature of the DRL grant process reasonably requires projects to commit to a very concrete set of objectives and a relatively long-term course of action to achieve them. Regrettably, the current nature of the Internet freedom space is one punctuated by crisis, (e.g. Arab Spring, Syria, etc.). At times these crises create situations where project resources could have more impact if they were diverted from stated plans to responding to the immediate situation on the ground.

There is a positive, but indirect, connection between DRL's Internet freedom portfolio and the expansion of civic freedom within authoritarian regimes.[62] The analysis of five different case studies revealed that the effect that Internet freedom has on political space is dependent on the level of Internet penetration, the reach of the Internet freedom programs, and the regime's repressive capacity. It is also worth noting that non-political uses of the Internet can transition into politicized online mobilization. In other words, the expansion of online social space can at times inadvertently lead to greater political space. This suggests that promoting Internet freedom regardless of whether it helps activists can ultimately result in greater political space. DRL's projects seek to assure that all people have free access to the Internet, which could be a critical enabler that helps to empower opposition movements within repressive states.

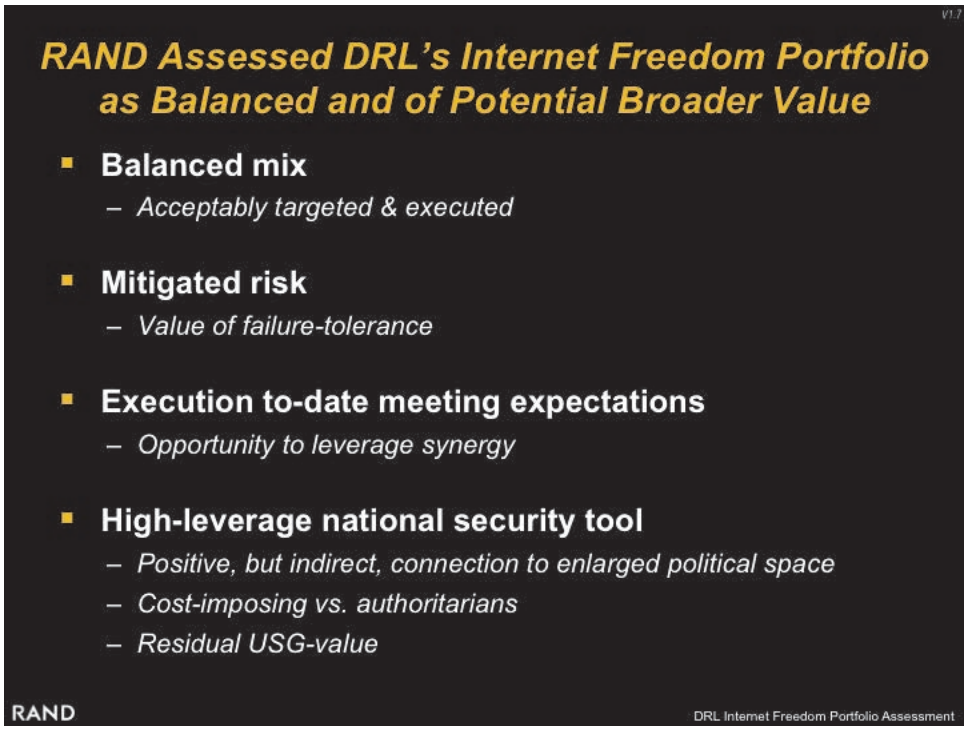
While access to the Internet has not proven to be decisive in successful revolutions, it has played a *critical enabling role*. Given that the Internet greatly reduces the traditional barriers of distance and time, it facilitates the sharing of information. Therefore, at times Internet access has de-stabilized authoritarian regimes by generating information cascades, which in turn have drawn a greater number of protesters to demonstrations. Access to the Internet also enables opponents to challenge a government's version of an event by creating and disseminating alternative interpretations that may resonate with others. In sum, the ability to anonymously express dissent online and coordinate the actions of a group can help to create new opposition movements and expand the appeal of existing dissident groups.

[62] This section is drawn from Tkacheva, et al., 2013.

There are a number of tradeoffs that need to be considered when funding Internet freedom projects. One can seek to expand political space in different ways. On the one hand, increasing the absolute number of individual who choose to circumvent censorship would result in a net increase in political space. On the other hand, Internet freedom programs could focus on an elite group of agenda setters—bloggers, online journalists, and opposition leaders—by providing them with and teaching them how to use sophisticated anonymity, circumvention and communications technologies. In other words, the first strategy prioritizes broadening Internet freedom for all users, while the second strategy chooses to deepen online opposition by assisting a small number of activists. History suggests that at times the actions of a small group of committed activists can serve as the catalyst for regime change, and that they can have a disproportionate effect on outcomes. On the other hand, netizens who are not politically motivated and far outnumber the few committed activists can under the right circumstances become politically active, and decisively tilt the balance of power against a regime.

Similarly, DRL's Internet freedom program needs to find the right balance between generally improving Internet freedom and providing support to dissidents during a crisis. The former will generally improve peoples' lives by safeguarding a basic human right, while the latter has the potential to have a more significant and direct impact on political space. At different times, different combinations of strategies may be appropriate depending upon the specific context. In short, there is not a one-size fits all approach to promoting Internet freedom, but instead DRL needs to consider the particular environment and circumstances when determining how to best advance Internet freedom.

Finally there are some concerns about the U.S. government's Internet freedom programs. First, there is often a disconnect between those developing the circumvention and anonymity technologies and the societies that they hope will utilize these tools. Consequently, DRL needs to work to bridge this divide, by encouraging cooperation between non-governmental organization (NGOs) or country experts and the programmers developing Internet freedom technologies to improve the likelihood that the tools are tailored for and therefore embraced by a particular society. Additionally, there is a chance that the U.S. government could unintentionally discredit local activists who it funds. It is, therefore, important that DRL be mindful of this risk and take appropriate steps to reduce the chances that this occurs.



Through this assessment, RAND determined that DRL currently has a balanced and acceptable performing portfolio of Internet freedom programs. DRL's portfolio contains an balance between the four factors that influence Internet freedom and political space, and it also aligns with DRL's stated strategy. At the time of our assessment, no insurmountable obstacles in the execution of the portfolio were apparent. DRL has already taken steps to enhance synergy among its grantees. The structural issue of compensation for highly talented IT professionals is largely beyond the influence of DRL, and, therefore, is not easily remedied.

Moreover, portfolio risk, the cumulative performance, political, and security risk, has not yet to materialized, and we did not detect any currently imbedded flaws that would drive future risk significantly higher. That does not mean that unforeseen problems might not arise in the future. While individual projects will, in all probability, fall short in one aspect or another, the portfolio should still support DRL's Internet freedom strategy due to it's diversification.

DRL has a level of risk tolerance in assembling its portfolio of projects through a rigorous and competitive selection process[63]. It also diversified its portfolio to mitigate risk. This diversification was evident in its project investment allocation, geo-political focus, project

[63] Grants are competitively selected on quality of project ideas, program planning and ability to achieve objectives, cost effectiveness, program monitoring and evaluation, and the host institutions record and capacity.

breadth, differentiation of capabilities to be developed, and ambition of project objectives. DRL has maintained a degree of failure-tolerance within its portfolio, which ensures that it does not become too risk-averse and stagnant.

We assessed that, based on execution at the time of the assessment, the DRL portfolio has promise for making a positive contribution to State Departments Internet freedom initiative. This contribution could be enhanced by nurturing a community-of-interest of current, past, and potential future DRL grantees, which could collectively catalog and share lessons learned, best practices, and create a clearing house for Internet freedom tools. Such a community could also act in U.S. interest during times of crisis when Internet freedom capabilities might act as an accelerant to enlarging political space. The working and trust relationships built around the DRL portfolio might serve as a foundation, from which like-minded members could pool or integrate their expertise to rapidly respond to emerging opportunities to overcome Internet repression. Such voluntary efforts might have the agility to operate inside authoritarian regime's decision cycles, and would certainly be faster than formal USG programmatic responses. The high probability of tight alignment between USG interests and those of this community would significantly mitigate the normal political risks associated with such independent actions.

Beyond its value in facilitating a crisis response capability, the portfolio provides the USG a cost-imposing arrow in its national security quiver. Cost imposing strategies take a long-term approach, focus on asymmetries, and implement measures that capitalize on U.S. strengths, while exploiting adversary weaknesses.[64] Internet freedom targets repressive states' Achilles heel, that is their internal legitimacy.[65] These regimes demonstrate their concerns by devoting over 50% of their security budgets to internal security.[66] Because countries, like China and Iran, view Internet freedom as a critical threat, they are likely to continue to allocate a disproportionate amount of resources to trying to control the Internet as long as there are easy ways for their citizens to circumvent censorship and surveillance. Further, USG-funded Internet freedom portfolios are a somewhat unique cost-imposing capability—one that has a high-confidence alignment with USG public and private interest, and low-probability of being compromised or exploited.

Consequently, we believe that these second-order and unintended outcomes might be of equal, or greater, value to the USG compared to the Internet freedom portfolio's intended first-

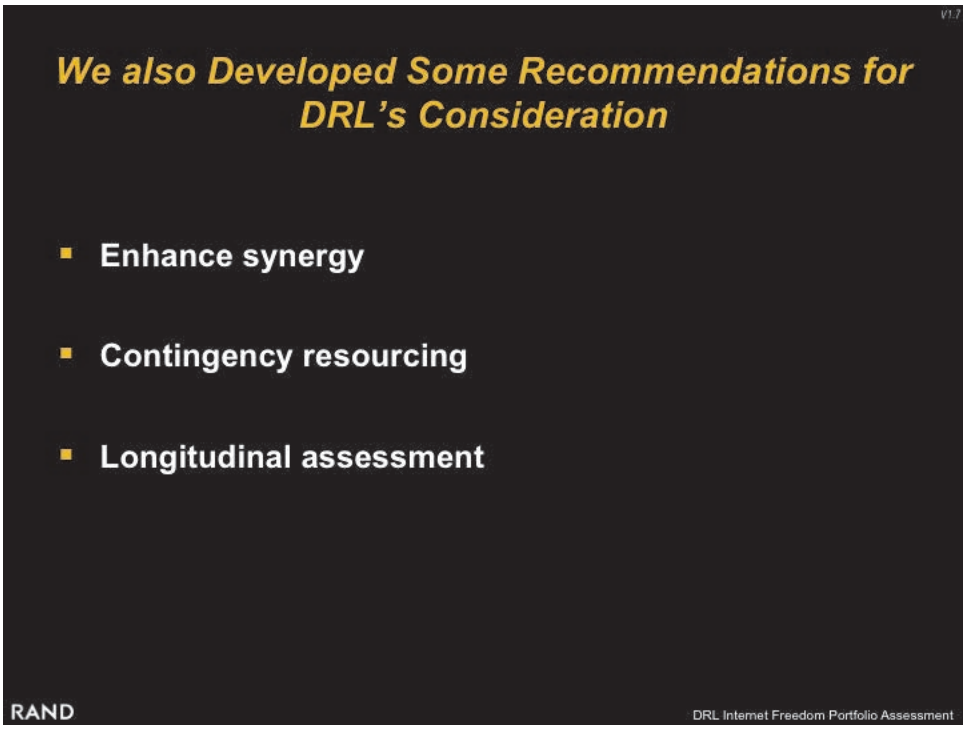
---

[64] For more information, see Thomas G. Manhken, ed., *Competitive Strategies for the 21st Century: Theory, History, and Practice*, Stanford, Calif.: Stanford University Press, 2012.

[65] Robert G. Sutter, *Chinese Foreign Relations: Power and Policy Since the Cold War, Lanham,* Md.: Rowman and Littlefield Publishers, 2012*,* p. 17; Office of the Secretary of Defense*, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013,* U.S. Department of Defense, 2013, p. 17; Keith Crane, Rollie Lai, and Jeffrey Martini, *Iran's Political Demographic, and Economic Vulnerabilities*, Santa Monica, Calif.: RAND Corporation, MG-693, 2008.

[66] Page, Jeremy, "Internal Security Tops Military in China Spending," *Wall Street Journal*, March 5, 2011; Jalil Roshandel, *Iran, Israel, and the United States: Regime Security vs. Political Legitimacy*, Santa Barbara, Calif.: Praeger Security International, 2011.

order objectives. In large part this is due to the fact that the community-of-interest and cost-imposing capabilities do not disappear when the current funding cycle ends. Rather they deliver a long lasting residual value to the USG.



As a result of our assessment we developed four recommendations for DRL to consider as their portfolio continues to mature. Our first recommendation, which DRL began to address during the course of the assessment, is to enhance the synergy within the portfolio and between its grantees. As discussed previously, this is the area we found that would provide the largest return on investment for DRL. It would allow them to increase the effectiveness of the entire portfolio, while decreasing its management/performance risk. Beyond merely providing opportunities for intra-portfolio collaboration, we also recommended that DRL create mechanisms to incentivize collaboration and that these be outlined in the request for proposals.

Second, we recommend that DRL consider a mechanism for contingency tasking. This recommendation grew from the observation that several of the projects were actively seeking ways they could leverage their DRL funds or their work for DRL to respond to the rapidly deteriorating situation in Syria. Because a key value of the DRL portfolio is the network that it helps to build, creating a funding mechanism to rapidly allow that Internet freedom community to act during a crisis could be a very effective use of DRL's resources.

Third, we recommend that DRL consider this assessment as a rigorous first-look at their portfolio, but that to fully realize its value, this process should be repeated over time. This is a one-time assessment, which accurately represents a snap-shot of DRL's Internet freedom portfolio in fiscal year 2012-2013. But as we have discussed, circumstances and strategies change—often very rapidly in this arena. Therefore, the Internet freedom portfolio needs to be periodically re-assessed to monitor its response to these changes and ensure that it is still optimized to achieve the State Department's objective of expanded political space.

Bibliography

Anderson, Collin, "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran," June 18, 2013. As of February 24, 2014: http://arxiv.org/pdf/1306.4361v1.pdf

Baer, Daniel, Deputy Assistant Secretary, Bureau of Democracy, Human Rights, and Labor, "Promises We Keep Online: Internet Freedom in the Organisation for Security and Cooperation in Europe (OSCE) Region," Statement Before the Commission on Security and Cooperation in Europe (U.S. Helsinki Commission), Washington, D.C., July 15, 2011. As of February 24, 2014: http://www.state.gov/j/drl/rls/rm/2011/168684.htm

Chomiak, Laryssa and John P. Entelis, "The Making of North Africa's Intifada," in David McMurray and Amanda Ufheil-Somers, eds., *The Arab Revolts: Dispatches on Militant Democracy in the Middle East*, Bloomington, Ind.: Indian University Press, 2013.

Conrad, Edward D., Michael D. Michalisin, and Steven J. Karau, "Measuring Pre-Adoptive Behaviors Toward Individual Willingness to Use IT Innovations," *Journal of Strategic Innovation and Sustainability*, Vol. 8, No. 1, June 2012, pp. 81-92.

Crane, Keith, Rollie Lai, and Jeffrey Martini, *Iran's Political Demographic, and Economic Vulnerabilities*, Santa Monica, Calif.: RAND Corporation, MG-693, 2008. As of February 24, 2014: http://www.rand.org/pubs/monographs/MG693.html

Dalkey, Norman Crolee, *The Delphi Method: An Experimental Study of Group Behavior*, Santa Monica, Calif.: RAND Corporation, RM-5888-PR, 1969. As of February 24, 2014: http://www.rand.org/pubs/research_memoranda/RM5888.html

Dickinson, Elizabeth, "Internet Freedom: The Prepared Text of U.S. Secretary of State Hillary Rodham Clinton's Speech, Delivered at the Newseum in Washington, D.C.," *Foreign Policy,* January 21, 2010. As of February 24, 2014: http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom

Diebert, Ronald and Rafal Rohozinski, "Beyond Denial: Introducing Next Generation Information Access Controls," in Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., *Access Controlled: The Shaping Power, Rights, and Rule in Cyberspace*, Cambridge, Mass.: MIT Press, 2010. As of February 24, 2014: http://mitpress.mit.edu/sites/default/files/titles/content/9780262514354_sch_0001.pdf

Dingledine, Roger, Nick Mathewson, and Paul Syverson, "Deploying Low-Latency Anonymity: Design Challenges and Social Factors," *Security & Privacy, IEEE ,* Vol.5, No.5, September/October 2007. As of February 24, 2014: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4336287&isnumber=4336264

The Economist, "Cat and Mouse: How China Makes Sure Its Internet Abides by The Rules," April 6, 2013. As of February 24, 2014: http://www.economist.com/news/special-report/21574629-how-china-makes-sure-its-internet-abides-rules-cat-and-mouse

Elster, Jon, ed., *Rational Choice*, New York, N.Y.: NYU Press, 1986.

Faris, Robert and Rebekah Heacock, "Introduction," in Urs Gasser, Robert Faris, Rebekah Heacock, *Internet Monitor 2013: Reflections on the Digital World*, Cambridge, Mass.: Berkman Center for Internet and Society, December 12, 2013.

Faris, Robert and Rebekah Heacock, "Looking Ahead," in Urs Gasser, Robert Faris, Rebekah Heacock, *Internet Monitor 2013: Reflections on the Digital World*, Cambridge, Mass.: Berkman Center for Internet and Society, December 12, 2013., pp. 86-87.

Faris, Robert and Nart Villeneuve, "Measuring Global Internet Filtering," in Ron Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge, Mass.: MIT Press, 2008.

Figliola, Patrcia Moloney, *Promoting Global Internet Freedom: Policy and Technology*, Washington, DC: Congressional Research Service, May 26, 2011. As of February 24, 2014: http://fpc.state.gov/documents/organization/166789.pdf

Figliola, Patricia Moloney, Kennon H. Nakamura, Casey L. Addis, and Thomas Lum, *U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology*, Washington, D.C.: Congressional Research Service, January 3, 2011. As of February 24, 2014: http://www.fas.org/sgp/crs/misc/R41120.pdf

Fung, Brian. "The feds pay for 60 percent of Tor's development. Can users trust it?" Washington Post, September 6, 2103. As of February 24, 2014: http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/06/the-feds-pays-for-60-percent-of-tors-development-can-users-trust-it/

Galperin, Eva and Morgan Marquis-Boire, "Syrian Activists Targets with Facebook Phishing Attack," *Electronic Frontier Foundation*, March 29, 2012. As of February 24, 2014: https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack

Gephi, *The Open Graph Viz Platform,* 2012. As of February 24, 2014: https://gephi.org/

Google, *Google Take Action*. As of February 24, 2014: http://www.google.com/intl/en/takeaction/

Gurr, Ted Robert, *Why Men Rebel?: Fortieth Anniversary Edition*, Boulder, Colo.: Paradigm Publishers, 2011.

Hanson, Fergus Baked In and Wired: eDiplomacy@State, Washington, DC: Brookings, October, 25, 2012.

Helmer-Hirschberg, Olaf, *Systematic Use of Expert Opinions*, Santa Monica, Calif.: RAND Corporation, P-3721, 1967. As of February 24, 2014: http://www.rand.org/pubs/papers/P3721.html

International Telecommunications Union, *The World in 2013: ICT Facts and Figures*, 2013. As of February 24, 2014: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Joseph, Sarah, "Social Media, Political Change, and Human Rights," *Boston College International and Comparative Law Review,* Vol. 35, No. 1, January 1, 2012, pp. 145-150.

Kelly, Sanja, "Despite Pushback Internet Freedom Deteriorates," in Sanja Kelly et al., *Freedom on the Net 2013: A Global Assessment of Internet and Digital Media*, Washington, D.C.: Freedom House, 2013.

Kelly, Sanja, and Sarah Cook, eds., *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*, Washington, D.C.: Freedom House, April 18, 2011.

Kelly, Sanja, Sarah Cook, and Mai Truong, eds., *Freedom on the Net 2012: Global Assessment of Internet and Digital Media*, Washington, D.C.: Freedom House, 2012.

Landree, Eric, Richard Silberglitt, Brian G. Chow, Lance Sherry, and Michael S. Tseng, *A Delicate Balance: Portfolio Analysis and Management for Intelligence Information Dissemination Programs,* Santa Monica, Calif.: RAND Corporation, MG-939, 2009. As of February 24, 2014: http://www.rand.org/pubs/monographs/MG939.html

Lewis, Alan A., *The Use of Utility in Multiattribute Utility Analysis*, Santa Monica, Calif.: RAND Corporation RAND Paper P-6396, , RAND, Santa Monica, 1980. As of February 24, 2014: http://www.rand.org/pubs/papers/P6396.html

Linbach, Mark I., *The Rebel's Dilemma*, Ann Arbor, Mich.: University of Michigan Press, 1998.

Lum, Thomas, Patricia Moloney Figliola, and Matthew C. Weed, *China, Internet Freedom, and U.S. Policy,* Washington, D.C.: Congressional Research Service, July 13, 2012. As of February 24, 2014: https://www.fas.org/sgp/crs/row/R42601.pdf

Lynch, Marc, *The Arab Uprising: The Unfinished Revolutions of the New Middle East*, New York, N.Y.: Public Affairs, 2013.

MacKinnon, Rebecca, *Consent of the Networked: The Worldwide Struggle for Internet Freedom,* New York, N.Y.: Basic Books, 2012.

Manhken, Thomas G., ed., *Competitive Strategies for the 21st Century: Theory, History, and Practice*, Stanford, Calif.: Stanford University Press, 2012.

Morozov, Evgeny, *The Net Delusion: The Dark Side of Internet Freedom,* New York, N.Y.: PublicAffairs, 2011.

Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, U.S. Department of Defense, 2013. As of February 24, 2014: http://www.defense.gov/pubs/2013_china_report_final.pdf

Olson, Mancur, "The Logic of Collective Action in Soviet-Type Societies," *Journal of Soviet Nationalities*, Vol. 1, No. 2, Summer 1990.

Open Net Imitative, *Profiles: China,* August 9, 2012. As of February 24, 2014: https://opennet.net/research/profiles/china

Page, Jeremy, "Internal Security Tops Military in China Spending," *Wall Street Journal*, March 5, 2011. As of February 24, 2014: http://blogs.wsj.com/chinarealtime/2011/03/05/internal-security-tops-military-in-china-spending/

Reporters Without Borders, *Enemies of the Internet 2013 Report: Special Edition Surveillance*, Paris, France, 2013.

Phys.org, "Factors Identified that Influence Willingness to Use Technology," March 8, 2013. As of February 24, 2014: http://phys.org/news/2013-03-factors-willingness-technology.html

Raub, Werner and Chris Snijders, "Gains, Losses, and Cooperation in Social Dilemmas and Collective Action: the Effects of Risk Preferences," *Journal of Mathematical Sociology*, Vol 22, No. 3, 1997.

Roshandel, Jalil, *Iran, Israel, and the United States: Regime Security vs. Political Legitimacy*, Santa Barbara, Calif.: Praeger Security International, 2011.

Schmidt, Eric and Jared Cohen, "The Digital Disruption: Connectivity and the Diffusion of Power," *Foreign Affairs*, Vol. 80, No. 6, November/December 2010.

Silberglitt, Richard and Lance Sherry, *A Decision Framework for Prioritizing Industrial Materials and Research and Development,* Santa Monica, Calif.: RAND Corporation, MR-1558, 2002. As of February 24, 2014: http://www.rand.org/pubs/monograph_reports/MR1558.html

Silberglitt, Richard, Lance Sherry, Carolyn Wong, Michael Tseng, Emile Ettedgui, Aaron Watts, and Geoffrey Stothard, *Portfolio Analysis and Management for Naval Research and Development*, Santa Monica, Calif.: RAND Corporation, MG-271-NAVY, 2004. As of February 24, 2014: http://www.rand.org/pubs/monographs/MG271.html

Shirky, Clay, "The Political Power of Social Media: Technology, the Public Sphere, and Political Change," *Foreign Affairs*, Vol. 90, No. 1, January/February 2011.

Sutter, Robert G., *Chinese Foreign Relations: Power and Policy Since the Cold War*, Lanham, Md.: Rowman and Littlefield Publishers, 2012.

Tkacheva, Olesya, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini, and Caroline Baxter, *Internet Freedom and Political Space*, Santa Monica, Calif.: RAND Corporation, RR-295-DOS, 2013. As of February 24, 2014: http://www.rand.org/pubs/research_reports/RR295.html

U.S. Department of State, *Internet Freedom*, undated. As of February 24, 2014: http://www.state.gov/e/eb/cip/netfreedom/index.htm

Zickuhr, Kathryn, *Who's Not Online and Why*, Pew Research Center, September 25, 2013.

Zittrain, Jonathan and John Palfey, "Internet Filtering: The Politics and Mechanisms of Control," in Ron Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, Mass.: MIT Press, 2008.