USAID
FROM THE AMERICAN PEOPLE

# WORKING WITH INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) IN DEMOCRACY, RIGHTS AND GOVERNANCE (DRG) ASSISTANCE PROGRAMS IN HIGHLY CONSTRAINED ENVIRONMENTS

**OCTOBER 2013**

This publication was produced for the United States Agency for International Development by Management Systems International.

# WORKING WITH INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) IN DEMOCRACY, RIGHTS AND GOVERNANCE (DRG) ASSISTANCE PROGRAMS IN HIGHLY CONSTRAINED ENVIRONMENTS

MSI MANAGEMENT SYSTEMS INTERNATIONAL
A SUBSIDIARY OF COFFEY INTERNATIONAL, LTD

coffey international development

600 Water Street, SW, Washington, DC 20024, USA
Tel: +1.202.484.7170 | Fax: +1. 202.488.0754
www.msiworldwide.com

Contracted under AID-OAA-I-IO-00002. Order No. AID-OAA-TO-11-00035

**DISCLAIMER**
The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

# CONTENTS

**TABLES**

# EXECUTIVE SUMMARY

The field of democracy assistance is being rapidly transformed by the introduction of new information and communication technologies (ICT). New programs frequently feature at least one ICT component, and many rely on ICT to facilitate or achieve key strategic objectives.

However, because ICTs are constantly changing, and because the intersection of democracy, rights and governance (DRG) and ICT is relatively new, both program planners and donors lack a common framework for employing various forms of ICT in different DRG interventions. In highly constrained political environments, a common analytical approach becomes even more important to ensure effectiveness and the safety of participants.

This guide is intended to serve as a framework for assessing the effectiveness of ICT in highly constrained programming environments. It can enable due diligence with respect to the risks and rewards involved in applying particular information technologies. The guide can also be used as a tool in designing programs, reviewing proposals, or monitoring/evaluating the progress of projects.

The framework here walks users through several steps in thinking about DRG objectives and ICT, including considerations of access, information flow, risk, and actors. The guide features checklists of due diligence questions, and provides suggestions for different ways to use the framework.

Ultimately, this guide does not aspire to keep abreast of every relevant technology trend. Rather, it seeks to provide durable and easy-to-use rules of thumb for DRG program designers, evaluators, and donors seeking to better understand and employ ICTs in these environments.

# I. PURPOSE OF THIS GUIDE

The field of democracy assistance is being rapidly transformed by the introduction and incorporation of information and communication technologies (ICT). This term is intended to encompass what is widely thought of as social media – technologies that enable information sharing and collective action – while not necessarily excluding such older digital technologies as websites, email, and so on. For the purposes of this guide, it will not include older ICT such as broadcast and print media.

New programs frequently feature at least one ICT component, and many rely on ICT to facilitate or achieve key strategic objectives.  For instance, some advocacy programs may feature websites that enable geographically separated program participants to communicate in a secure fashion. Others may involve the distribution of technology to specific users to facilitate information exchange and reporting on, say, rights abuses.  Still others may simply introduce ICT to the widest possible population group in the hopes that civil society will adopt, and adapt, the technology in ways best suited to their particular needs.

At the same time, because ICT are constantly changing, and because the intersection of democracy, rights and governance (DRG) and ICT is relatively new, both program planners and donors lack a common framework for evaluating the risks and rewards of employing various forms of ICT in different DRG interventions. In highly constrained political environments, a common analytical approach becomes even more important to ensure that the technology supports the goals and does not undermine the safety of participants.

Thus, this guide is primarily intended to serve as a framework for assessing the effectiveness (including usefulness and feasibility) of ICT given the nature of highly constrained programming environments and the desired program objective. The guide should also enable due diligence with respect to the risks and rewards involved in applying particular information technologies.  The guide can serve as an analytical tool for use in designing programs, reviewing proposals, or monitoring/evaluating the progress of projects using ICT in highly constrained environments.  It will provide general rules of thumb for projects featuring ICT in these environments, and will attempt to address new tools and proposed new tools, as well as existing, off-the-shelf technologies.

This guide may be used by both donors and implementing partners. Donors may find it particularly useful as a tool to evaluate proposals and to monitor the ongoing use of ICT in projects. Partners may want to use the guide for program planning purposes, as well as a way to better understand how donors may seek to gauge the effectiveness of employing ICT in their projects.

What this guide does *not* seek to do is evaluate or endorse particular technologies. ICT change rapidly, as do their uses and applications in projects, so by necessity this guide will not focus on providing up-to-date information on various technology applications. Rather, it seeks to provide users with rules of thumb for understanding categories of ICTs that typically feature in DRG programming in highly constrained environments. While it cannot address every specific situation, it should provide users with a more systematic way to analyze a particular project or environment.

"Highly constrained environments," as defined here, refers to situations in which states deliberately and significantly limit citizens' rights. It does not refer to conflict/failed state environments in which rights abuses stem from lack of governing authority. While these environments are also suitable for programming that involves ICT, they are beyond the scope of this guide.

At the same time, the ICT addressed in this guide can also be relevant to crisis situations that may arise within such highly constrained environments. In other words, in the event of a possible political transition and/or other political flashpoint situation, ICT normally used for particular DRG applications in a stable environment may be scaled up to be used by a wider population. Thus, the guide will help users think through the “scaleability” of various ICT categories in the event of such situations.

Before proceeding to the analytical framework, this guide will first introduce essential initial considerations relevant to DRG programs using ICT. These include common DRG objectives, various types of highly constrained environments, and the characteristics and pertinence of various forms of ICT.

# II. TYPICAL DRG OBJECTIVES IN HIGHLY CONSTRAINED ENVIRONMENTS

Generally speaking, there are three levels of project impact that DRG programs in highly constrained environments seek. The first is high-level impact, sometimes known as a Development Objective in USAID parlance. These are relatively broad impacts, and it can be difficult to attribute specific results to assistance programs. The second level is the outcome-level impact, generally referred to by USAID as an Intermediate Result. Most project proposals are geared toward this level of impact. The third, lowest-level impact is the project output level. This is the most easily quantifiable and attributable to specific projects, but may lack broader DRG significance.

DRG programs in highly constrained environments are typically looking to achieve certain types of high-level impacts. These broad, country-level impacts may look like the following:

- Citizenry is able to participate in democratic debate and discussion
- Citizens have access to diverse sources of information & analysis about events, issues, government decision-making and decisions
- Increased and more inclusive participation of citizens in social, political and economic life
- Human rights are increasingly safeguarded and respected

In order to conceptualize and operationalize such sweeping concepts, these DRG impacts can be further separated into lower-level outcomes, or intermediate results. For the purposes of this guide, these can be separated into three main categories: Knowledge and Information; Advocacy and Organizing; and Rights Protection. In non-constrained environments there are many more categories of activity available, including work on local governance, the rule of law, etc. However, since highly constrained environments typically do not permit such types of work, they are not included here. Under each category, several illustrative outcomes are listed. These outcomes are meant to represent longer-term goals, and do not necessarily include specific DRG objectives during crisis or political transition situations.

- Knowledge and Information:
  - Increased access by citizens to diverse sources of information
  - Expanded transparency about government deliberations, policies and laws
  - Enabling environment encourages the production of independent news (may include citizen journalism and other non-traditional forms of news production)
  - Increased popular awareness of DRG-related information, principles and ideas
  - Improved media literacy among activists and the general population

- Advocacy and Organizing:
  - Strengthened research, investigative and analytical skills among CSOs and the general public
  - Consensus-building and dialogue processes promote peaceful agreement on democratic rules and frameworks

  - Enabling environment is increasingly supportive of CSO formation, operation, civic activism
  - Improved organizational capacity, networking and advocacy among CSOs and other groups (including informal and online-only citizen groups)

- Rights Protection:
  - Strengthened citizen knowledge of universal human rights and responsibilities, roles of government
  - Enhanced, secure linkages to international advocacy and human rights monitoring organizations
  - Improved capacity by CSOs, legal community and/or others to defend human rights

At the project level, the outcomes listed above are further disaggregated into specific outputs that contribute to those outcomes. DRG programs that utilize ICT may include such project outputs as:

- Providing training in DRG-related skills and issues, such as journalism, organizing, video production
- Enabling information collection, dissemination and analysis of DRG issues
- Enabling secure group discussion, or providing safe spaces for sensitive discussions
- Facilitating cooperative planning and action
- Maintaining routine, timely and/or real-time secure communication for CSOs, activists and the general public
- Gauging public sentiment
- Enabling production of, and access to, alternative domestic, exile and diaspora media

While the sample outputs, outcomes and impacts are meant to cover the general categories of objectives usually found in DRG programs operating in highly constrained environments, they are not meant to be exhaustive.

# III. CLASSIFYING HIGHLY CONSTRAINED ENVIRONMENTS ACCORDING TO THEIR TREATMENT OF TECHNOLOGY

Highly constrained environments interact with technology in different ways, and the type of ICT used in programming should be adjusted accordingly. According to Roosevelt University professor David Faris, who has conducted studies of these types of regimes, highly constrained environments can be grouped loosely into three major categories: “response regimes,” or relatively permissive environments; “control regimes,” or semi-permissive environments, and  “restrictive regimes” (or “7&7 regimes,” as Faris calls them, so named because they typically rank last in Freedom House’s rankings of press freedom and civil liberties).[1] A brief description of these types, and countries that exemplify them, follows.

*Response regimes*, according to Faris, tend to allow unlimited access to major political sites on the internet, but harass individual activists. In these cases, digital activists drive the public agenda on certain

[1] Faris, David.  “Social Media and Democracy Promotion.” PowerPoint presentation. Management Systems International, Washington D.C. July 25, 2012.

issues, and the regime is forced to respond after the fact. Examples of this type of highly constrained environment include Egypt and Tunisia before their political transitions.[2]

*Control regimes* take a more proactive approach toward monitoring, censoring and otherwise grappling with information technology, says Faris. These regimes block most political content and prevent access to sites used by activists, such as YouTube. Citizens of these countries become adept at using proxy servers or other methods of accessing blocked content, and in moments of political crisis, the general public can use unblocked sites to mobilize. Examples of these types of regimes include current day Iran and Vietnam.[3]

*Restrictive regimes* are, as the name indicates, the most authoritarian in their treatment of technology, denying many if not most usage of social media to the population while also potentially using technology to monitor citizens. In these regimes, access to the internet is tightly controlled, with violent repercussions for offenders. Activists tend not to use electronic media, scaling up to SMS in crisis situations. North Korea is an example of one of these environments.[4]

It is important to understand the differences between highly controlled environments because not all constraints on information technology are the same, and different technologies may have different impacts, and repercussions for users, depending on the political environment. For instance, Faris points out that, if activists are primarily interested in increasing the safety and anonymity of the politically active, an acceptable approach to use in a control regime would be to use an anonymous online identity in online applications, whereas in a 7&7 restrictive regime activists should take the additional measure of using anonymizing proxies and other approaches that serve to obfuscate the link between the information provider and the end-user at the network level).

This guide is primarily concerned with control regimes, which are less constrained than restrictive regimes but not as permissive as a response regime might be.  In other words, control regimes likely:

Allow mass access to ICT (i.e. cell phones, internet), but block most political content

- Do not attempt to block most or all social networking sites or applications that are not overtly political
- Track activists' use of technology, and cracks down on individual activists or dissidents to make a point
- Grow more restrictive and resembles a restrictive regime during times of political crisis or transition
- Make some attempt to proactively use technology to track dissident or civil society activity
- Feature laws and regulations governing ICT that make it a crime to access or use ICT for specific political purposes (although language may be left vague)

[2] Ibid.
[3] Ibid.
[4] Ibid.

# IV. CHARACTERISTICS OF DIFFERENT TYPES OF ICTS AND THEIR PERTINENCE TO DRG OBJECTIVES

This section will outline the major categories of ICT that typically feature in DRG programs. Note that this guide is **not** intended to provide an up-to-date listing of specific technologies, as the nature of technological change means that individual technologies will quickly outpace the guide. Nor can it possibly be comprehensive. Rather, what will be presented here are broad categories of ICT that are relevant from a DRG standpoint, and that may assist in making determinations as to the suitability of different types of ICT for different purposes.

One of the most important ICT characteristics, for the purposes of this guide, is the general direction of information flow that it encourages. Generally speaking, we can think of the various ICT as primarily facilitating or encouraging top-down, bottom-up, or horizontal (peer-to-peer) information flow. Top-down ICTs typically encompass older forms of technology such as broadcast radio and television, or newspaper publishing, as well as newer forms of publishing where information is disseminated by a central source, such as an online publication, to large groups of people. Bottom-up ICTs generally serve to aggregate and redistribute information from large portions of the population; examples might be crowdsourcing or crowd mapping applications. Horizontal information flow typically encompasses older technologies such as email and SMS, as well as social media and its various offshoots, which encourage a “many-to-many” style of communication. In constrained environments in particular, horizontal flows can be conceptualized in three ways: (1) allowing information in; (2) allowing information out; and (3) facilitating information within the country.

These information flow characteristics can impact what types of technologies are appropriate for different types of DRG objectives, which will be addressed in the analytical framework portion of the guide. They also have implications for the level of risk borne by participants in a DRG program, which will also be addressed in the analytical framework. Various ICT may also encourage more than one direction of information flow.

In the table below, different forms of ICT are loosely categorized according to their purpose. The various purposes listed here can be relevant, in varying circumstances, to different DRG objectives. The following list enumerates these categories, describes the predominant information flow direction(s) associated with each category, notes the possibility of open-source adaptation and innovation within this category, categorizes the potential risk level, and gives developed country examples.[5]

| **Purpose** | **ICT Forms** | **Information Flow** | **Open-source compatible** | **Risk level to user in control regime** | **Example** |
|---|---|---|---|---|---|
| Publishing | Websites, Blogs, Microblogs, Wikis, Hybrids (i.e., email publishing, Speak-to-Tweet, etc.) | Top down, horizontal, bottom up | Yes | Medium, depending on familiarity with anonymizing software | Blogger, Drupal/ WordPress-based sites |

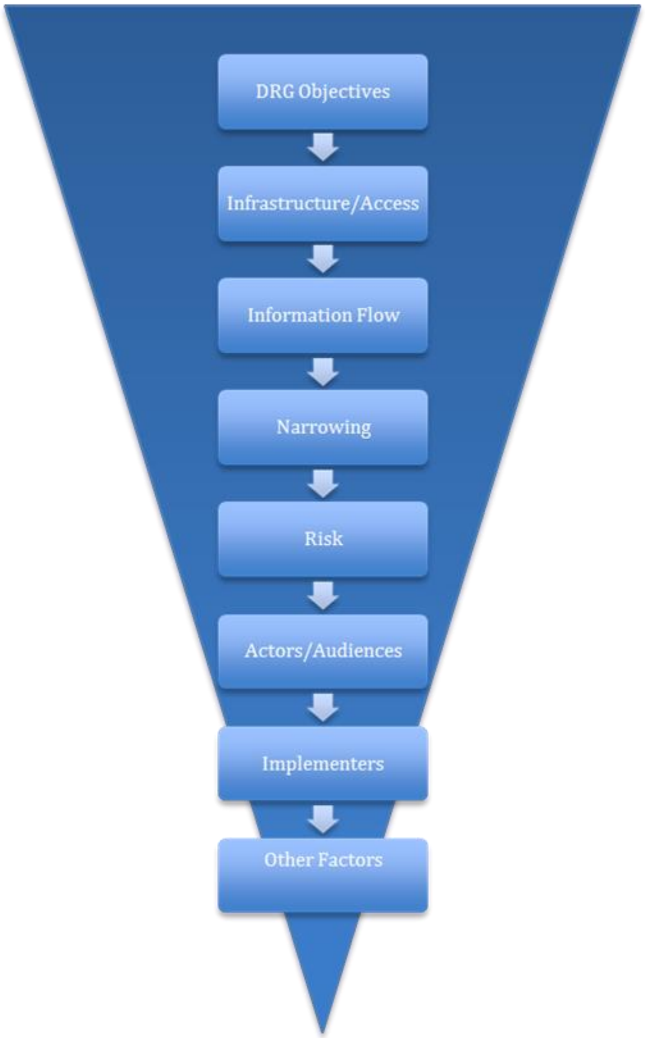
[5] Categories are adapted from “Social Media Landscape 2011” http://www.marywisemandesign.com/social-media-landscape/. Accessed 9/20/12.

| | | | | | |
|---|---|---|---|---|---|
| Networking | Professional, social, mobile | Horizontal | Not particu-larly | High | LinkedIn, Facebook |
| Location/ spatial | Location-based social media, mapping | Bottom-up, horizontal | Some-what | Very high | Foursquare, OpenStreet Map, Ushahidi |
| Content sharing | Music, video, photo, documents, including cloud-based file-sharing | Horizontal | Yes | High | Flickr |
| Asynchron-ous discussion | Email, listservs, web forums, blog comments, SMS, various forms of text and video chat | Top-down, Horizontal | Yes | Medium, depending on anonymizing capabilities of users | 4chan, Slashdot, Skype chat |
| Realtime dialog | Video, audio, and /or text, direct person-to-person calls or one-to-many broadcasts | Horizontal, top-down | Yes | Medium to high, depending on anonymizing capabilities of users | SMS/MMS, Skype, Google Hangouts, Adobe Connect |

## V. ANALYTICAL FRAMEWORK

The analytical framework presented here is designed to help donors, program planners, and program evaluators think through the implications of the use of different forms of ICT to achieve DRG objectives. Because technology changes so quickly, it cannot reasonably hope to point guide users toward a specific technology that is appropriate for particular programs. However, by following the analytical process outlined here, funders, planners and others should be able to think logically about the how difference between different forms of ICT in different highly constrained environments, and make informed decisions about potential impact.

Narrowing options to select an ICT solution:



In addition to the desired objective, the country environment and the expected flow of information, all introduced earlier, these steps incorporate consideration of additional key factors such as audience, risk profile and implementer capacity.

In nearly every step, key questions are posed in order to help elicit the information necessary to make informed decisions about ICT use relative to DRG objectives, context and available ICT tools. Some of these questions will be more relevant for donors seeking to evaluate programs proposing specific ICTs for specific purposes; others may be more relevant from a program design perspective that is, starting with an environment or DRG objective and then matching that objective with an appropriate ICT to leverage impact.  Users of this guide should select among these sample questions as appropriate.

The answers to these questions do not necessarily determine a particular project design vis à vis ICT: each of the factors discussed here must be evaluated and weighted, relative to the other factors, so that possible trade-offs are clearly understood.  Notably, certain ICT may appear to yield the greatest impact on desired objectives (in the short term), but carry more risk than is acceptable to program participants and sponsors. Other forms of ICT may be both secure and capable of reaching a broad population, but not suitable for specific target populations, such as rural women, for instance. Program planners must be clear about the intended purpose of the ICT and whether or not they intend the ICT in question to be scalable in the event of a political crisis; if so, the ICT's direct relevance to the target population may be offset by the potential for the ICT to be available to the wider population in the eventuality of a political opening, etc. (For more on scalability, please see Step Eight (Other Factors) below.

## Step One: DRG Objectives

In many if not most cases, the DRG objectives for a particular highly constrained environment have already been identified through a separate analytical process or assessment. As noted in Section II, these objectives can be broadly divided into three categories: Knowledge and Information; Advocacy and Organizing, and Rights Protection, with specific objectives illustrated above.

However, not all DRG objectives may be suitable for an ICT component. Too often, ICT are vaguely attached to every objective, whether or not they enhance or help achieve the desired impact. Thus, from a programming perspective, the first task is to determine which DRG objectives, of the ones that have already been identified, are best suited to an ICT component.

### Key questions to consider

- Are ICT necessary to achieve the objective?
- Will the introduction of ICT leverage the impact of work on this area in ways not possible otherwise?
- Conversely, could the introduction of ICT distract from, or otherwise impede, achieving results?
- Are the risks inherent in introducing ICT for the objective outweighed by the potential DRG benefits to the population or targeted group?
- Can the introduction of ICT for this particular objective be scaled up in the event of a political crisis to prove of benefit to the broader population?
- If ICT are introduced to achieve this objective, will longer-term impact of the initiative be determined by the lifetime of the technology? For instance, if a particular social networking technology accompanies a long-term advocacy/organizing objective, will results be hampered if the technology is compromised by state authorities or becomes out of date?

## Step Two: Infrastructure and Access

The type of infrastructure present (including technological infrastructure as well as "soft" infrastructure, e.g. legislation or regulations regarding ICT), as well as the factors shaping the population's access to technology, are important in understanding what types of ICT may be most suitable to the environment. DRG-related groups, in particular, may not be able to use typical channels of information exchange, or the types of ICT used by the majority of the population, due to risk and other factors.[6]

Considering cases may help illustrate these points. For instance, Country A, a control environment featuring widespread use of non-smartphone cell phones but limited access to the broadband internet, would present a different DRG environment than Country B, a control regime with widespread access to wired and wireless broadband.  If a project proposes to introduce a broadband-reliant information portal (i.e., one including lots of pictures, video, and other heavy bandwidth applications) targeting the general population in the case of Country A, then the project is not taking the country's infrastructure and access patterns into account.

[6] While not covered by this paper, it is worth noting that traditional media usually not an option for DRG groups, as they tend in highly constrained settings to serve less as means for information exchange than a one-way, state-sponsored mechanism.

Moreover, it is important to understand who accesses what kind of ICT. It may be that the general population in Country A relies on SMS for news and information, but that human rights activists are more sophisticated ICT users who use proxies to get around censorship. In this case, a DRG program with a more narrow focus on improving the organizing capacity of human rights activists might make use of web-based social media for organizing, such as Facebook, Twitter, or a local platform. However, it would also need to take into account and potentially mitigate the risk to those users.

In this step, then, it is important to focus not just on technological infrastructure but the non-technological structural factors (i.e., regulations, sociological determinants) that in turn affect access and usage of ICT. The following questions are designed to help evaluators, program designers and others better understand these dynamics in the environment in question.[7]

### Key questions to consider

- Technological infrastructure:
  - How does the majority of the population exchange information: word of mouth, print, radio, TV, internet, cell phone, or some other platform?
  - What type of infrastructure exists for each type of medium? Is the infrastructure for each medium up to date, and progressing apace with the speed of technological change? Why or why not?
  - Where does local capacity exist to operate, repair, and replace new infrastructure, and how might this be supported?
  - What are the key trends with respect to digital convergence? Is this affecting how the majority of people obtain information?

- Non-technological infrastructure:
  - What structural, political, regulatory, economic, or other factors are helping or hindering access to ICT?
  - What are the laws and regulations governing ICT? Do laws and regulations restrict the flow of information, and if so, how?
  - How would one characterize the business and economic environment surrounding ICTs? Is there a domestic ICT industry, and how might it be characterized?

- Patterns of access and usage:
  - What is the status of key telecommunication indicators for the country in question? What do they tell us about access to information?
  - Can the population in general access, create and share digital content? Are there clusters of expertise that can help the general population access, create and share digital content?
  - What is the capacity level of the general population in using various ICT? What is the capacity level of dissidents and activists? Where might capacity building have the greatest impact?
  - Is the population at large familiar with the use of ICT to access politically sensitive information? What about civil society organizations?
  - Does civil society generally practice self-censorship when using ICT?
  - Of the major sub-groups targeted by the DRG intervention, how do their access and patterns of usage differ? Why?
  - How much do these sub-groups trust different types of ICT?

[7] A portion of these are adapted from Kalathil, Shanthi, *Developing Independent Media As An Institution of Accountable Governance: A How-To Guide*, The World Bank, 2011.

- What are the risks to individual users, both activists and non-activists, in using ICT to access politically sensitive information?
- Where would a targeted intervention have the most impact?

## Step Three: Information Flow

At this point, the analytical framework should have helped to sharpen the focus on DRG objectives, environment, and the factors that shape access and usage. Now, it is necessary to narrow the universe of options by considering the direction(s) of information flow suggested by key DRG objectives, as well as the ICT associated with those information flow directions.

In this chart, illustrative ICT are associated with the sample DRG objectives provided earlier, each placed in the information flow category or categories *most likely* to be associated with it. Again, while this cannot be exhaustive, it should help users of this guide picture the types of DRG initiatives most likely to be associated with certain directions of information flow, and the ICT in turn associated with those directions.

| | **INFO FLOW** | | |
|---|---|---|---|
| **DRG OBJECTIVES** | **Top Down** | **Horizontal** | **Bottom Up** |
| ***Knowledge and Information:*** | | | |
| Increased access by citizens to diverse sources of information | Websites, blogs | Mobile networking, social networking, file-sharing, listservs, SMS | Wikis, Location-based social media, mapping, microblogs |
| Expanded transparency about government deliberations, policies and laws | Websites, blogs, | Social networking, file-sharing, listservs, SMS | Microblogs, wikis |
| Enabling environment encourages the production of independent news and information | Websites, blogs, | File-sharing, listservs | Wikis |
| Increased popular awareness of DRG-related information, principles and ideas | Websites, blogs, | Games, mobile networking, social networking, file-sharing, listservs, SMS | Microblogs, wikis |
| Improved media literacy among activists and the general population | Websites, blogs, microblogs | Mobile networking, social networking, file-sharing, listservs, SMS | Wikis |
| ***Advocacy and Organizing:*** | | | |
| Strengthened research, investigative and analytical skills among CSOs and general | Websites, blogs | File-sharing, listservs, SMS, | Wikis, live-mapping, crowd-sourcing applications |

| | | | |
|---|---|---|---|
| public | | | |
| Consensus-building and dialogue processes promote peaceful agreement on democratic rules and frameworks | | Mobile networking, social networking, listservs | Wikis |
| Enabling environment is increasingly supportive of CSO formation, operation, civic activism | Websites, blogs | | |
| Improved organizational capacity, networking and advocacy among CSOs and other groups (including informal and online-only citizen groups) | | Mobile networking, social networking, professional networking, file-sharing | Live-mapping, crowdsourcing apps, location-based social media, risk mitigation tools (data-stripping, face-blurring, de-linking tools) |
| ***Rights Protection:*** | | | |
| Strengthened citizen knowledge of universal human rights and responsibilities, roles of government | Websites, blogs, microblogs | Mobile networking, social networking, file-sharing | Location-based social media, mapping, wikis |
| Enhanced, secure linkages to international advocacy and human rights monitoring organizations | | Mobile networking, social networking, professional networking | Microblogs, risk mitigation tools (data-stripping, de-linking) |
| Improved capacity by CSOs, legal community and/or others to defend human rights | Websites, blogs, microblogs | Mobile networking, social networking, professional networking, file-sharing | Location-based social media, mapping, wikis |

## Step Four: Synthesizing Analysis to Narrow the Universe of ICTs

By asking key questions about objectives, environment, infrastructure and patterns of use, and combining those insights with the information in the preceding table, the program evaluator or designer should now have a better grasp of what types of ICT are likely to be well-suited to the DRG objective(s) at hand. Applying the insights gained thus far allows us to focus our further analysis on a smaller subset of ICT solutions.

For instance, if the DRG objective is to increase popular awareness of DRG-related information, principles and ideas, then one would consider the environment (control environment, with perhaps additional specificity depending on current events), the infrastructure of the country, general patterns of usage, and the ICT suited to particular directions of information flow associated with that objective. If considerations of usage patterns show that many people have access to desktop computers and broadband, that might point one in the direction of websites, blogs, wikis, and other publishing-related social media (top-down, to disseminate ideas), as well as toward networking applications (so that information can spread from peer to peer), perhaps blending the two.

Similarly, if the DRG objective is to improve organizational capacity, networking, and advocacy among civil society organizations, then one would again consider the environment, the infrastructure and patterns of usage as well as the ICT suited to that objective. Let's say that a survey of infrastructure and patterns of usage indicates that most people exchange information through SMS and other cell phone applications, while access to broadband is sparse. One might consider some type of mobile social networking application in such a situation.

## Step Five: Actors/Audiences

After this initial narrowing exercise, consider the specific actors targeted by the DRG intervention, and evaluate the likelihood that they will use the subset of ICT in question. For instance, is the DRG program primarily aiming to reach the general public? Political activists? Or another sub-group, such as youth, women, a regional population, or workers in a particular industry?

Consideration of sub-group matters because there can frequently be considerable geographical, demographic or other variation across populations.  Youth, for instance, may be most easily reached through gaming, which might include some type of civic education component.  Depending on the nature of the highly constrained environment, women may not have access to all forms of ICT: for instance, they may be more likely to access a cell phone than a home or public computer with broadband. Other sub-groups may also have better access to some forms of ICT over others.

Once the primary group or groups have been isolated, one can then consider a number of key questions to further illuminate appropriate ICT programming decisions.

### Key questions to consider

- How would you describe the ICT literacy of the group targeted by the DRG intervention? This may include: familiarity with various forms of ICT; access to ICT; willingness to use new/complex tools.
- Does the targeted group have access to technical support or expertise? Is the group connected to the open source community? Lack of technical support and/or connections to developers may hamper uptake and real utilization of the ICT.
- How has the group used ICT in comparable situations in the past? Did such use of ICT lead to favorable outcomes? Why or why not? What does this indicate about this group's ability to make productive use of the ICT being considered?
- Has usage of the particular ICT being considered arisen organically among the targeted group? I.e., is this a technology that the group is already using to some extent and simply requires scaling up and/or modification to allow the group to use it more effectively? Or is an entirely new ICT being introduced? Newly introduced ICT are less likely to be adopted by the target group. The most successful DRG/ICT interventions will build upon an organically developed/used ICT to scale up impact.
- If a new ICT is being introduced, what is the likelihood that the group will adopt the ICT being considered? Does the group need the ICT to accomplish its goals (i.e., is the group asking for the technology, or is it someone else's idea)? Include considerations of infrastructure, access, familiarity/comfort, patterns of use, willingness to assume risk.

- Is use of the ICT under consideration by this group likely to prove sustainable over the long term? Consider legacy costs, ongoing operating costs, and the cost of any upgrades required in the future. What is the local availability of service, parts, etc. and can the targeted group access these services?
- What future regulatory changes might impact the target group's ability to make use of the ICT? What other structural elements (business climate, telecommunications regulatory environment, free speech legislation, security environment) might impact the group's ability to make use of the ICT for DRG purposes?
- Is this group likely to be able to scale up usage of this ICT in the event of a political crisis? Why or why not?

## Step Six: Risk Factors

In a highly constrained environment, use of any ICT poses distinct risks to the users and/or other beneficiaries of the technology. Funders and implementers of such programs must be aware of those risks, make sure participants are aware of those risks, and do their best to mitigate them (while seeking to preserve the effectiveness of the DRG intervention).

Many governments in control or restrictive environments actively censor information, restrict use of ICT, and use ICT to monitor individual users. They can do so in several ways, including any combination of the following:

- **Bandwidth throttling**: keeps data volume low to limit the amount of traffic that can be sent over the internet- can make high-volume service like streaming video practically unusable;
- **IP blocking**: prevents all packets going to or from targeted IP addresses;
- **Traffic classification/ shallow packet inspection**: more sophisticated than IP blocking, this can halt any request sent through a given protocol, such as FTP, BitTorrent, streaming video;
- **Packet fingerprinting**: more refined than shallow packet inspection, it looks not only at packet header but at length, frequency of transmission, and other characteristics;
- **Keyword list blocking / deep packet inspection**: the most refined method for blocking internet traffic, it examines not only a packet's header but its payload, giving the ability to filter packets at a surgical level – requests/responses featuring certain keywords can be dropped or an error message returned;
- **Domain name system poisoning**: intentionally misdirects user's request to another IP address. This can be used to impersonate a system and capture sensitive information, or to proxy the request and capture information going to/from the service to the user;
- **Countrywide intranet**: essentially creates a "safe" intranet for the entire country, with no connection to the global internet.[8]

It should be noted here that while users in such countries develop means to avoid these measures, governments keep developing new censorship and monitoring tools as well. Thus, this guide cannot list the most up-to-date measures undertaken either by the populace or by governments.

Country examples help illustrate these issues. Iran, for instance, has a wide base of internet usage, with approximately 43% of respondents to a 2012 BBG/Gallup poll reporting they had access to the internet in their household. [9] The country's filtering and monitoring system is one of the most extensive in the world.

[8] Figliola, Patricia Maloney, Kennon H. Nakamura, Casey L. Addis, Thomas Lum. "U.S. Initiatives to Promote Global internet Freedom: Issues, Policy, and Technology." April 5, 2010. Congressional Research Service.

[9] "BBG Research Series Briefing: Iran Media Use 2012," June 12, 2012. http://www.bbg.gov/wp-content/media/2012/06/BBG-Iran-ppt.pdf Accessed 1/21/13.

The government also restricts access by limiting the speed of internet access that ISPs can provide to households and public access sites, making it one of the only countries in the world to do so. This makes downloading multimedia content extremely difficult, and blocks off entire portions of the global internet to the Iranian population. Iranian bloggers must obtain licenses, and blogger arrests following the 2009 disputed elections point to an increasingly sophisticated monitoring system. Despite all these issues, however, the Iranian blogosphere is quite vibrant.[10]

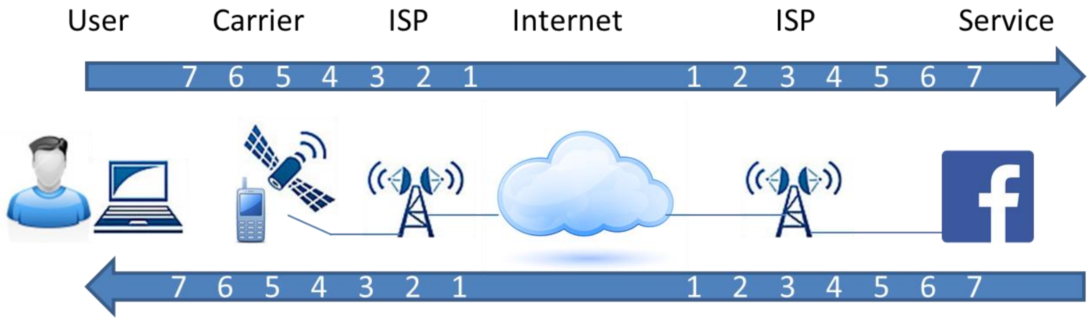
While all ICT are risky, some are associated with higher risk than others, depending upon the nature of the technology and the ways in which the technology is being used. The chart below uses the Open Systems Interconnection (OSI) model to show vulnerabilities at various stages of the flow of a request through the network. This helps in developing an assessment of the risk of an approach in a control regime.

**Vulnerabilities at various levels of the network stack**[11]

| | | OSI Layer | Function | Attack |
|---|---|---|---|---|
| **Host Layers** | **Data** | 7. Application | Process data, interface with user | Viruses, Worms, application weaknesses allowing access to underlying data and administrative controls, impersonation |
| | | 6. Presentation | Encryption/Decryption, conversion between data formats | Key substitution attacks |
| | | 5. Session | Interhost communications | Man-in-the-middle attacks where data are intercepted on their way to/from user and host |
| | Segments | 4. Transport | End-to-end connections, reliability and flow control | Denial attacks like TCP sync flooding, UDP flooding; Exploratory attacks like port scanning |
| **Media Layers** | **Packet** | 3. Network | Path determination and logical addressing | IP modification, DHCP attack, ICMP attack, DNS poisoning |
| | Frame | 2. Data Link | Physical addressing | MAC modification, MAC attack, MAC flooding |
| | **Bit** | 1. Physical | Media (cabling, wireless signal) and binary transmission | Physical interception by tapping cabling or monitoring wireless traffic en route |

[10] Ibid.

[11] After http://en.wikipedia.org/wiki/OSI_model

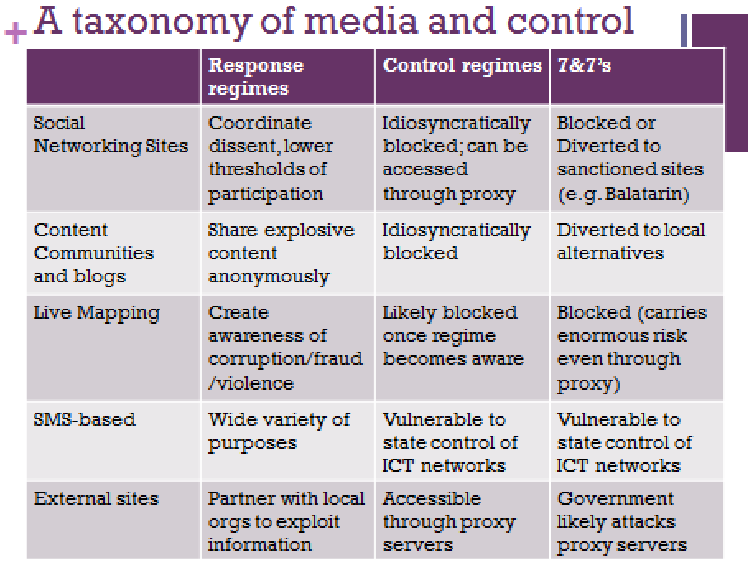


As we see in the diagram, requests flow from users down through the OSI stack 7-1 and then up through the OSI stack 1-7 on the other end (the service they are trying to use, or sometimes a user on the other end, as with an SMS message). Then the service responds, sending a corresponding message back through the same flow 7-1, 1-7. Each step represents an opportunity for attack. An attack may provide the adversary access to information being sent, information about the location of the sender, and/or information about the identity of the sender. Access to one of these elements may expose one or more of the others. Users of networked services in highly constrained environments must therefore develop habits and countermeasures to protect against adversaries gaining:

- Access to information
  - Blog posts may provide information about the interests and associations of a subject to his/her adversaries.
  - Adversaries may gain this information by masquerading as a legitimate user, or by accessing system resources illicitly by breaking into the system as a user, system administrator or network administrator.
- Access to location (realtime or historical)
  - Cell networks can provide adversaries fairly accurate information about the whereabouts of a known account. Using a cell phone linked to recurring payment information like a credit account can provide adversaries with a history of an individual’s movements.
  - Approximate location of wired connections can be determined for internet use.
  - Posting pictures of events from cell phones or later through traceable accounts on sharing sites can provide adversaries with evidence of participation or interest in prohibited or sensitive activities.
  - Use of crowd mapping sites may provide useful information to adversaries about the location of a subject. If a subject reports incidents in a clustered area, an adversary may flag him/her for interest and attempt to discover his/her identity.
- Access to identity
  - Providing real, personally identifiable information when signing up for services like communities of practice, social organizing sites or professional organizations may provide an adversary a way to discover and trace information about an individual and their associates.
  - Accessing sensitive or prohibited systems/services while using an identified network account (recurring payment mobile or ISP-billed internet) can provide an adversary a way to trace behavior back to an individual.

If users assume that their information is subject to inspection through the whole transport stack, then it is obvious that encrypting the messages passing through the transport stack is critical to protecting themselves in a highly constrained environment. Using SSL, seen on the web as HTTPS, is a good approach as it provides good protection of information during transport from the user to the service. Once data or metadata is recorded in a system, then it may be available to adversaries who are able to penetrate that system. Therefore systems that encrypt data "at rest" are optimal. However, this level of security is extremely rare in public-facing systems where usually the only encrypted piece of information is the user's password (if that).

David Faris's chart below looks at different types of ICT and the ways they are controlled or blocked across the three different regime types. [12]



A taxonomy of media and control

| | Response regimes | Control regimes | 7&7's |
|---|---|---|---|
| Social Networking Sites | Coordinate dissent, lower thresholds of participation | Idiosyncratically blocked; can be accessed through proxy | Blocked or Diverted to sanctioned sites (e.g. Balatarin) |
| Content Communities and blogs | Share explosive content anonymously | Idiosyncratically blocked | Diverted to local alternatives |
| Live Mapping | Create awareness of corruption/fraud /violence | Likely blocked once regime becomes aware | Blocked (carries enormous risk even through proxy) |
| SMS-based | Wide variety of purposes | Vulnerable to state control of ICT networks | Vulnerable to state control of ICT networks |
| External sites | Partner with local orgs to exploit information | Accessible through proxy servers | Government likely attacks proxy servers |

Faris's chart demonstrates that the number and variety of ICT possible in control and restrictive regimes is significantly constrained. Donors and program planners should be aware that features such as content communities and blogs, even if not overtly focused on political objectives, may be idiosyncratically blocked (or monitored or attacked) by the regime. Programs should ideally have a backup plan - or two - for incorporating ICT in the event that the technology of choice is blocked or otherwise compromised by the regime and/or bad actors. Having a full-time ICT person on staff to respond with flexibility in the event of a compromised technology might be one way to anticipate and plan for difficulties, for instance. At the same time, it is not reasonable to expect human rights activists to suddenly transform themselves into technology experts, so donors must keep this in mind when evaluating projects.

There is no magic bullet when it comes to keeping ICT out of the hands of bad actors, whether they are state agents or those intent on using ICT to incite violence or hatred. Similar issues have often been raised in traditional media development programs with respect to older communication technologies such as radio or broadcast television. Putting any ICT into the hands of the community entails a degree of risk that the ICT will fall into the hands of those who will use it for anti-DRG purposes. While use of the ICT can be monitored, there is no way to "take back" a technology once it has propagated among a wider community.

### Key questions to consider

- What is the level of risk that the user is exposing him- or herself to by using a given technology to share information? Examples of risk levels are threats to: privacy, reputation, freedom, and life.

[12] Faris, David. "Social Media and Democracy Promotion." PowerPoint presentation. Management Systems International, Washington D.C. July 25, 2012.

Users should make informed decisions about the likelihood of a risk manifesting before using a technology to share information in a highly constrained environment.

- How well does the ICT being considered account for the risk profile of the environment in question? I.e., is the technology likely to "work" given a control or restrictive environment? Does the program take into account the ways use of the ICT might be compromised by the regime?
- How well do participants understand the nature of the risk when using the ICT in question? Have they used the ICT before?
- Does the plan allow for training and educating participants about the risks they are exposing themselves to in using the specific ICT, and how to mitigate those risks? I.e., is there a budget for training in, e.g., proxy servers, anonymizing software, etc.?
- Does the program implementer have a Plan B in the event that the ICT in question is compromised (censored, shut down, or monitored by the state; or seized by bad actors)?

## Step Seven: Implementation Factors

Not all implementing organizations have the same capacity when it comes to utilizing ICT for DRG programs. The organizations most likely to be successful will have deep in-country knowledge and a track record of successful ICT-related interventions.

There is often a trade-off between selecting an organization with the requisite DRG program experience, donor-relations savvy and technological skills, and an organization with credible expertise and roots in-country. Smaller in-country organizations, working organically with local civil society to design tools to fit specific needs, are most likely to identify ICT that will be used successfully by the target group. This is because these groups are in contact every day with the opportunities and constraints imposed by the target environment. Anecdotal evidence suggests that programs that take a top-down approach to introducing ICT are generally unsuccessful. However, small local organizations usually do not have the track record, experience with proposals/donors, governance structure, etc. to get them past the proposal evaluation stage with many international donors.

International implementing organizations, on the other hand, generally have more resources and familiarity with the aid process; thus, their proposals generally are more comprehensive, feature a greater facility with both DRG and ICT issues (particularly from a donor standpoint), and demonstrate the ability to provide tech support to participants if needed. However, unless they are working in close partnership with an in-country organization, they typically approach the fusion of ICT and DRG in a non-organic, top-down manner that may fail to take into consideration the likelihood of adoption by the target group and/or be driven by the need to appear "cutting edge." Even those that partner with local organizations (which is often extremely difficult in control or restrictive environments) may have difficulty with this.

Unfortunately, there is no easy solution to this conundrum. Donors may be able to nudge various organizations together, but the reality of any highly constrained environment may make local organizations distrust the legitimacy of outside organizations. Donors can also try to strengthen the capacity of local groups to undertake donor-funded projects, but this often involves a level of resource and time investment that is not always realistic or possible.

### Key questions to consider

- Does the implementing organization propose to introduce a new ICT, or to enhance the use of an existing ICT by a group that already uses it? If it proposes to introduce a new ICT, can it demonstrate that it has given sufficient thought to the likelihood that the group will adopt the ICT, given patterns of use, familiarity, risk, etc.?

- Does the implementing organization demonstrate a thorough understanding of the risk factors involved in the particular environment? How does it plan to mitigate risk to both participants and itself?
- Does the implementing organization have sufficient capacity (human, technological, managerial) for what it's proposing to accomplish with the ICT in question?
- Has the implementing organization considered the ease/difficulty of implementation with respect to ICT? How has it demonstrated this?

## Step Eight: Other Factors

A variety of other factors can influence the choice or suitability of the ICT being considered. These might include such issues as versatility, scalability, monitoring and evaluation, and innovation.
**Versatility** refers to the likelihood that the ICT could be used for both the targeted and other, unanticipated DRG uses. A website that contains fairly static information about human rights is unlikely to be versatile. On the other hand, if the comments to the website are designed in such a way to attract lively discourse among a broader population, then the ICT may contribute to a broader goal of fostering democratic dialogue.

**Scalability** also refers to the possibility of ICT being used in unanticipated ways, primarily by large numbers. Many innovative uses of ICT during situations of political crisis stem from the technologies being used for purposes other than their intended ones. So, for example, a professional networking site that is usually devoid of politics may become, in a moment of political crisis, a hub for broad civil society mobilization - particularly if it has been overlooked by the regime for being fairly innocuous in the past. It is difficult to predict what specific types of technology will "catch on" in moments of political crisis or transition, however. Particularly during such events, usage of technology hinges on many different factors, including ease of usage, access to ICT, security, and so on. Moreover, during such moments of crisis, technology usage is almost by definition organically driven, arising spontaneously as need dictates among the population.

Very generally speaking, the greater the scalability of the technology, the greater the regime's ability to use that technology for surveillance and other information-gathering purposes. Moreover, as David Faris notes, there is an issue with diminishing returns when moving from simple and scalable broad-public-use technologies, such as social networking sites, to more specific applications such as anonymizing technology. Thus, scalability generally diminishes when the technology's sophistication increases.[13] Faris posits a brief hierarchy of scalability with respect to commonly used technologies in authoritarian contexts:

- **Blogs/Websites**: default public, very easy to use/consume;
- **Social Networking Sites:** require little other than basic computer literacy, but also not fully public;
- **Livemaps/Collaborative Production Applications**: often require both basic computer/cell phone literacy as well as a kind of conceptual understanding of what exactly is being done; probably require an activist to "activate" a new user to participate in the use of these technologies;
- **Downloadable Circumvention Devices**: require comparatively advanced computer literacy + capacity for risk-taking and trust that the devices actually work.[14]

[13] Email conversation with David Faris, February 6, 2013.
[14] Email conversation with David Faris, February 7, 2013.

Each of these technologies, of course, comes with a component of risk that may or may not be fully understood by the broader population. Moreover, all of these categories should be taken with a grain of salt, in that they are highly context-dependent. With those caveats in mind, it is generally easier to rule out forms of ICT that are *not* likely to be used more widely during crisis. The following questions may help elicit more detailed thinking about versatility and scalability.

**Monitoring and evaluation** of ICT can be quite tricky in control or restrictive environments. The very factors that necessitate a DRG/ICT intervention are the ones preventing effective ongoing monitoring and impact evaluation. Some ICT lend themselves more easily to monitoring and evaluation than others; a DRG-related bulletin board system (BBS), for instance, can be monitored to see how many people post to the site, and how often, about what topics.  Many other ICT, however, are difficult to monitor, and care must also be taken not to compromise the safety of the participants. It is extremely important that an organization seeking to monitor a technology consider that putting in place detailed monitoring capabilities creates the risk that the regime may discover and exploit those same capabilities. Organizations should assess this risk against the possible benefits to be gained by monitoring a program in high detail.

Even when monitoring ICT is possible, it is frequently difficult to identify, and then collect, appropriate indicators. Even gathering detailed data on basic internet use in many countries, for instance, is difficult, much less assembling specific data points on usage, impacts, and so on. In non-constrained environments, there are frequently publicly available data points that can be used as proxies for more specific indicators: for example, one might track the number of journalists jailed as a proxy for broad press freedom. In highly constrained environments, however, this data may not be publicly available.
What tends to happen in highly constrained environments is a combination of precise data collection - i.e., monitoring numbers of users, messages, etc., when possible - with some form of context-driven qualitative assessment.  In these cases, it is also important to verify the reliability of the indicators obtained via technology, as this can also be manipulated by the regime or other actors for their own purposes.

Finally, it is important to note that while **innovation** can be both important and necessary in constrained environments, it is frequently misunderstood by donors or others seeking to apply technology for specific uses. Innovation may be as simple as pairing an “obsolete” technology - land-line telephones or pay phones, for instance - with a commonly used ICT, such as email. Combining different types of ICT can frequently bring additional benefits, either from a risk perspective (speak-to-Tweet) or from a DRG objective perspective (combining publishing with social networking, etc.). Innovation in these environments may also require considering multiple uses of older technologies, such as perhaps answering machines or fax machines. In other words, it is not *necessarily* exemplified by the newest technology with the most bells and whistles.

Moreover, the price of innovation is frequently failure, as Silicon Valley can attest.  Truly exploring new ideas is risky, something that donors frequently are unable to stomach. The challenge for donors and program implementers, then, is how to reward innovation, while also maintaining some level of impact. It may be that donors need to consider the concepts of innovation and impact somewhat separately; i.e., projects designed to reward innovation should do just that, placing a higher value on innovative experimentation and risk-taking (in an entrepreneurial sense) than on ultimate impact or long-term sustainability. It is also important to point out that the risks in highly constrained environments may be to individual physical safety as opposed to a simple loss of face.

### Key questions to consider

- Can the ICT in question be used for other DRG purposes in addition to its intended one? Is it likely to be used for other purposes, and if not, why not?
- Is the broader population familiar with the form of ICT in question? Is the technology easy for the general population to use? Does the ICT require special skills or special equipment to use?
- What are the factors (social, technological, economic, physical, or otherwise) enabling or hindering the usage of this technology by the broader population, and are these factors likely to shift in the event of political crisis or transition?
- If the technology in question appears only scalable to elites, is this also likely to be of value in the event of a political crisis?
- Does the general population have wide and easy access to this form of ICT? Is access likely to be curtailed by the regime in the event of crisis, and is the broader population likely to make the effort to continue to use the ICT in question if/when this does happen?
- Is the broader population likely to use this ICT when security concerns are at the forefront?
- Could use of this technology by the wider population compromise the safety of large numbers of individuals, perhaps unbeknownst to them? Are they likely to understand the risks involved?
- How well will we be able to monitor the use of this technology and determine if it is generating the desired results?
- If we are undertaking an innovative approach in the target environment, what factors are we aware of that would contribute to its success? What factors would contribute to failure?
- What would be the impact of failure on us and on our local partners/users?

## VI. CONCLUSION: EMPLOYING THE ANALYTICAL FRAMEWORK IN DIFFERENT WAYS

This analytical framework can be used for a number of purposes. While it unfolds in a linear fashion to walk users through technology choices and implications, it can also be used for proposal review, program monitoring purposes, thinking through the design of RFAs or RFPs, and so on.

For program design, the guide can be helpful in determining the family of technologies best suited to the political environment, the country context, the actors targeted and the DRG objective at hand. It is not meant as a step-by-step guide to DRG/ICT program design, nor as an exercise to identify the exact type of technology suited to very specific circumstances, but can aid in thinking through crucial questions that should feed into any effective program. For instance, someone designing a CSO capacity-building program with a gender focus in a highly constrained environment, and wondering what type of technology may boost the impact of the program, may find it useful to go through the steps of the guide to narrow the choice of ICT in question, as well as to understand the nuances, risks, potential benefits and drawbacks of incorporating that ICT.

The guide may also be useful when designing an RFA or RFP for particular DRG objectives and countries/region. The analytical framework can be used to winnow down the scope of an RFA/RFP, in order to receive more accurately targeted proposals. It can also be used to “reality check” the aims of an RFA/RFP that seeks to marry specific types of technology to DRG objectives.

Proposal reviewers can use the guide to assess program design, implementer strength, and appropriateness of proposed technology to the given the DRG objective and other contextual factors. They may find it helpful to work through the eight steps of the guide, if not for each proposal under review, then for each distinct DRG objective noted in the RFA or RFP. For instance, if the primary objective of the RFA is "Increased access by citizens to diverse sources of information," then one would keep this DRG objective, and the country context, in mind while performing the analytical steps of the framework to determine the family of technologies best suited to the country or region in question. For more of a shorthand approach, proposal reviewers might simply wish to use the "key questions to consider" in each section to identify proposal strengths and weaknesses. If a number of organizations have presented very similar proposals, the Key Questions in Step Seven, Implementation Factors, may help distinguish between different organizations' implementing capacity.

For program monitoring purposes, parts of the analytical framework can be used to understand whether or not a specific ICT may be contributing to an ongoing program's impact. For instance, if users want to understand if a certain technology is reaching its intended audience and achieving the intended impact, they can walk through the questions in Step Five. If users want to better understand ongoing or changing risks associated with the technology, they may wish to go through the questions in Step Six.