Conference Report
February 2014

What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World

Rapporteur: Cynthia Romero

USAID
FROM THE AMERICAN PEOPLE

About the Rapporteur

Cynthia Romero is senior program officer for Latin America at Freedom House. Ms. Romero has over a decade of policy and programming experience, with expertise in civic participation, freedom of expression, and youth engagement in Latin America and Eurasia. She has previously worked at the Atlantic Council, the National Democratic Institute, and the U.S. Senate. Ms. Romero was the rapporteur of the Atlantic Council report *Georgia in the West: A Policy Road Map to Georgia's Euro-Atlantic Future*, co-chaired by Senators Jeanne Shaheen and Lindsey Graham, and is a frequent commentator on Spanish- and English-language media.

Acknowledgements

This report reflects the findings of a gathering in Mexico City on securing human rights defenders, during which over 60 activists, policymakers, donors and implementers engaged in productive debate and shared their expertise. Freedom House would like to thank all of the participants for their frank and insightful contributions. In particular, we are grateful to Arjan Van der Waal, Daniel O'Clunaigh, Josh Haynes, and Kevin Sturr for providing substantive edits to the report. Thanks to Katie Striffolino, Shauna Dillavou, Ela Stapley, David Loxton, Daniel O'Clunaigh, and Boniface Mwangi for allowing us to feature information about their innovative work in the report, as well as all of those who featured their tools and tactics at the conference. From the Freedom House team, Mary McGuire, Chloe Schwenke, Daniel Calingaert, and Danilo Bakovic provided expert analysis and guidance, which enriched the substance of the conference and this report. Raquel O'Byrne, Meagan Allen, and Geysha Gonzalez coordinated logistics with ease and professionalism, which ensured successful outcomes at the conference. Special thanks to John Ewing for editing the report. This report was made possible by the generous support of the U.S. Agency for International Development (USAID).

Executive Summary

Around the world, governments and non-state actors are using sophisticated techniques to monitor, threaten, and harass human rights defenders (HRDs) and journalists. The growing use of digital technology has empowered activists to rally citizens around common causes and hold governments accountable, but it has also opened new doors for surveillance and harassment of activists and citizens' activities online. On November 14–15, 2013, Freedom House, funded by the United States Agency for International Development (USAID), held a global conference in Mexico City entitled "What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World,"[1] which brought together over 60 policymakers, donors, and activists to explore the full range of emerging threats and best strategies to overcome them; take an honest look at what is and is not working; and chart a path forward for more proactive and realistic solutions to build the resilience, sustainability, and relevance of HRDs and their movements. The conference sought to answer "what's next?" by identifying opportunities that can be exploited to build up frontline defenders and their ability to uphold human rights principles fearlessly and strategically at home and abroad.

Among the key findings were the following:

- HRDs are facing a shifting political landscape in which restrictions against their work rapidly evolve and threats arise from state and non-state actors. To push their agenda ahead, HRDs, implementers, and donors must focus on contingency planning and put systems in place to prevent attacks and reprisals rather than responding after the fact.
- Digital security tools are useless if they are not introduced with proper accompaniment so that trainers can assess beneficiaries' needs and risk profiles, and help activists think robustly about changing their online and offline behavior and implementing protocols to safeguard themselves. Donor funds should be geared towards replicating and localizing existing tools and making sure they are used responsibly, rather than creating new tools.

- Activists face a range of threats that go beyond digital attacks, including physical threats and intimidation that can also cause psycho-social harm, as well as legal and fiscal restrictions that require specialized counsel. Security trainers need to build up a minimum of knowledge in all of these areas in order to effectively strengthen activists' self-protection capabilities.

- Collaboration is essential to get ahead of the game, and almost 100 percent of implementers surveyed indicated that they will collaborate in some form with others. However, most of these implementers indicated that barriers, including distrust among CSOs and donor policies that disincentivize collaboration, often make collaboration difficult.

The following recommendations emerged from the findings:

- HRDs should systematize what they learn in security trainings to be proactive when thinking about their security and that of their organizations. They should also replicate what they learned with others in their network and be inclusive by sharing these tactics more broadly with those who may be at risk, including women HRDs, LGBTI groups, youth activists, and other communities facing similar challenges.

- Activists should harness technology and the arts to build public support for their human rights causes, create self-protection networks, and seek allies to avoid being isolated by authoritarians.

- Implementers should invest resources into establishing a more holistic approach to security training and assistance that addresses HRDs' physical, digital, psycho-social, and other vulnerabilities.

- Implementers and donors must "walk the talk" on security by incorporating security protocols into their own internal practices. For donors, walking the talk also means never shying away from publicly espousing human rights principles as a core of foreign policy and development aid, and as a key talking point when engaging with repressive regimes.

- Donors and implementers should focus less on funding new digital security tools and more on training HRDs in the use of existing tools, with an emphasis on changing behaviors that put them at risk and thinking proactively about contingency planning and security protocols.

- Donors should use coordinated bilateral engagements with countries in which HRDs and other targeted populations are under attack to stress the state's responsibility to protect these populations. Foreign assistance to these countries should be conditioned on, and provide support for, their implementation of measures to protect targeted populations.

- Donors should restructure funding policies to prioritize and integrate security in all programming and incentivize collaboration among donors and implementers.

Overview

Around the world, governments and non-state actors are using sophisticated techniques to monitor, threaten, and harass human rights defenders (HRDs) and journalists. The growing use of digital technology has empowered activists to rally citizens around common causes and hold governments accountable, but it has also opened new doors for surveillance and harassment of activists and citizens' activities online. With support from the U.S. Agency for International Development (USAID), Freedom House held a global conference in Mexico City on November 14–15, 2013, entitled "What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World,"[2] which brought together over 60 policymakers, donors, and activists to explore the full range of emerging threats and best strategies to overcome them; take an honest look at what is and is not working; and chart a path forward for more proactive and realistic solutions to build the resilience, sustainability, and relevance of HRDs and their movements. Participants engaged in highly interactive discussions and exercises designed to elicit collaborative and innovative answers to "what's next?" by identifying opportunities that can be exploited to build up frontline defenders and their ability to uphold human rights principles fearlessly and strategically at home and abroad. The host location of Mexico provided a perfect backdrop to address these questions as the location of one of Freedom House's largest programs bolstering protections for journalists.[3] This report summarizes the key findings and proposes recommendations from the conference.

"Urlaub 2005 – México" by http://www.flickr.com/photos/schlaeger/ is licensed under http://creativecommons.org/licenses/by/2.0.

Rationale

As illustrated in Freedom House's *Freedom in the World 2014* report, global freedom has been in decline for eight consecutive years. This is due in part to the rise of authoritarian internationalism,[4] in which authoritarians increasingly collaborate in order to roll back internationally accepted human rights norms, at home and abroad, that stand in the way of their efforts to concentrate power and satiate the interests of elites.

On the domestic front, authoritarians trade worst practices to restrict HRDs that seek to hold them accountable, including sharing surveillance technologies and intimidation tactics, as well as sophisticated legal and fiscal restrictions to criminalize civil society organizations (CSOs) and restrict freedom of expression, assembly, and association. In response, the U.S. and other democratic countries have sought to support HRDs in pushing back against these restrictions. However, the latest revelations of the U.S. government's mass surveillance programs have put into question the prevalence and purpose of surveillance by democratic states, hurt U.S. credibility as a proponent of Internet freedom, and strengthened claims of a double standard by authoritarians who purport they too surveil HRD activity because of national security.

To avoid complying with human rights standards that check their authority on the international stage, authoritarians also seek to undermine the jurisdiction of international and regional institutions, as recent attacks against the Inter-American Commission on Human Rights and Kenya's efforts to withdraw from the International Criminal Court illustrate. While authoritarian voices are united in challenging the authority and legitimacy of international mechanisms that might hold them accountable, democratic countries are at best ambiguous about investing in these institutions and, at worst, complicit in asserting that the international community should not interfere in domestic affairs. Authoritarian regimes also play on the non-intervention principle to criminalize international cooperation and foreign assistance to HRDs, as evidenced by the termination of direct USAID and other donor programming in Russia, Bolivia, and elsewhere. Unfortunately, many democratic countries have failed to push back on these creeping restrictions, and to articulate a response that reinforces human rights promotion as an essential core of their foreign policy and development strategies.

While authoritarian regimes are emboldened to pursue unchecked power and avoid domestic and international accountability, HRDs and their democratic supporters around the world are struggling to promote universal human rights, retain popular support for these values, and uphold the responsibility of the international community to hold governments accountable to these norms. Many human rights activists and international support groups are vulnerable, underfunded, and adrift on how to safely, sustainably, and effectively advance their causes—and protect themselves while doing so. Although international donors and human rights organizations, including Front Line Defenders, Freedom House, and many others, offer rapid response emergency assistance that provides a vital lifeline to HRDs and CSOs under attack, emergency support funding is limited and, therefore, primarily reactive and short-term. Moreover, so long as foreign donors do not engage in forceful diplomatic challenges against

authoritarian laws criminalizing foreign assistance, CSOs risk reprisal when they accept financing and support from these donors.

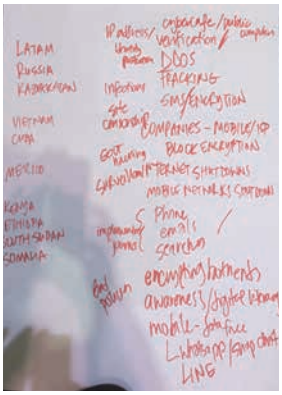
Many HRDs have found innovative ways to stay safe in the face of attacks, fight back against restrictions, and gain popular support for their causes. However, although international solidarity exists among those advancing human rights, the human rights community has not tapped into its comparative expertise and lessons learned to capture these success stories and use them to put forth proactive and holistic protection strategies to build the resilience, sustainability, and relevance of HRDs and their networks. In response, Freedom House sought to answer the following question: What have we learned from the latest wave of authoritarianism, and how do we use what we learned to get ahead of the game and ensure the survival and sustainability of human rights and those working to advance them? During the conference, we set out to pursue the following objectives:

- To better understand how practices and policies by foreign donors, implementers, and HRDs themselves inadvertently make them more vulnerable.
- To articulate proactive, achievable, and relevant solutions to tackle the digital, physical, psychological, and other vulnerabilities of HRDs, including women, youth, and LGBTI HRDs.
- To craft a roadmap that lays out strategic parameters to overcome the vulnerabilities and exploit the strengths of HRDs, including women, youth, and LGBTI HRDs.

Findings

Emerging Threats

In recent years, journalists, human rights defenders, and activists around the world have harnessed the many advances in online and digital technology to better organize citizens, promote transparency, and hold governments accountable to universal human rights standards. In response, those governments around the world who feel threatened by being judged by such standards have unleashed restrictions on freedom of expression, assembly, and association, and they are becoming more sophisticated and tech savvy in their efforts to monitor, threaten, and harass activists, particularly in the aftermath of the Arab Spring. In collaboration with like-minded governments and transnational companies, authoritarian regimes are employing advanced hacking and surveillance practices, coupled with traditional intimidation tactics. Efforts to restrict and even demonize human rights work have left HRDs vulnerable to physical, rhetorical, and online attacks (including slander, beatings, death threats, and killings). Repressive regimes are also employing certain traditional cultural values that undermine any non-domestic role by women to undercut the work and safety of women HRDs. As documented in *Freedom of the Press* and *Freedom on the Net*, governments are becoming more aggressive in their tactics to crowd out spaces for free expression in traditional and online media. Such governments are also imposing sophisticated fiscal and legal burdens, including onerous registration and tax regulations and restrictions on funding sources, to make it impossible for CSOs to operate and garner much-needed foreign assistance.



Activists in rural settings and/or closed societies where Internet access was once restricted are starting to have greater access to the Internet in recent years, but many of them are ill-equipped and uninformed about the risks they face online, or continue to face gender-based constraints on access to the Internet. The feeling of being free online for first-time Internet users can lead to risky online behavior that undermines their security. Using popular but unsecured applications, such as Skype, WhatsApp, and BlackBerry Messenger, as well as social media sites like Twitter and Facebook, have become second nature for many activists who do not realize the extent to which these sites can expose their identity, location, and other sensitive information. From crackdowns against microbloggers in China to killings and death threats against citizen journalists in Mexico, online novices are under attack and unaware of potential assistance and support they can receive from traditional HRDs and international support groups. In Latin America and other regions, many of these threats and acts of violence are originating from non-state actors, including organized crime. While in some countries, such as Mexico and Colombia, governments are beginning to publicly acknowledge their responsibility to protect citizens against these threats and implementing protection laws and state protection mechanisms, a history of widespread impunity in these countries undermines the credibility of these efforts.

In repressive regimes where the state is the primary source of attacks against HRDs, it is unfortunately common for citizens to be apathetic, or worse, supportive of government efforts to curtail and repress human rights activism. At times, HRDs pursue effective international advocacy to hold their governments accountable to human rights norms but struggle to mobilize domestic support for human rights at the grassroots, resulting in low public approval or interest in their efforts. In many countries, particularly those with high anti-West sentiment, government-led smear campaigns paint HRDs as elite, Western-funded interest groups that do not represent the daily concerns or values of citizens, or as troublemakers causing social unrest. In the face of government-led efforts to discredit their work and an onslaught of intimidation and violence, many HRDs are constantly under attack, are struggling to remain active, and are being challenged by public attitudes to demonstrate that their activism is relevant and valuable.

As youth activists, women's groups, and the LGBTI community become better organized to advance their rights, they are also becoming the target of attacks. In many conservative societies, women and LGBTI activists are not only subject to attacks from governments but also from the general public that do not view their universal human rights claims as legitimate and are resistant to allowing them a voice and a space to articulate and demand such rights. As a result, they are marginalized and prone to violence and harassment. In many countries, youth activists have been at the forefront of social protests and, as a result, are prime targets of government crackdowns. While youth activists are adept at using social media and other tactics to organize en masse, many of them lack the skills or resources to protect themselves effectively when they come under attack. Conference participants found that many of these challenges, as well as the unique tactics that these groups have employed to confront attacks, are underrepresented in discussions on HRDs. Traditional HRDs have little awareness or understanding of the diverse challenges and vulnerabilities that these emerging groups face, and there is scarce collaboration or exchange of best practices between these groups and traditional HRD communities. Moreover, a tendency to refer to these groups as "vulnerable populations" is not only disempowering but also fails to reflect the strength and resilience these communities have exhibited in the face of reprisals and lack of public understanding or empathy. Thus, fostering greater collaboration and understanding between these populations and traditional HRDs will not only help to mainstream understanding about these communities and their needs but also offer traditional HRDs fresh approaches on how to pursue strategies that are innovative, resilient, and sustainable.

Challenges and Gaps in Protection Efforts

Conference participants identified the following challenges and gaps in protection efforts to overcome the emerging threats described above.

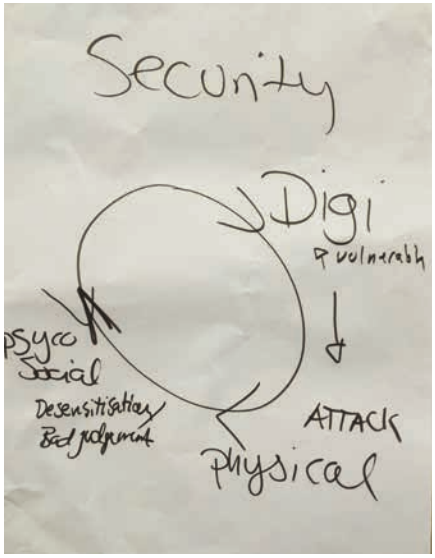
- **Protection efforts are reactive.** Participants recognized that one of the principal challenges to overcoming and protecting against the emerging threats is that HRDs, implementers, and donors alike realize the importance of security *after* they or a colleague, partner, or grantee are under attack (at which point their identity, work, communications, etc., may already be compromised). Although the international donor community has provided more funding in recent years for security training and assistance, beneficiaries seek help once they have been the subject of an attack. Most organizations providing assistance, either in the form of security training and/or emergency assistance, end up focused on helping beneficiaries respond to and prevent further attacks, rather than on preventative contingency and security planning to build resilience and establish protocols to avoid attacks in the first place. Building such protection capacity within segments of local human rights movements, as Protection International has done, is the exception for now.

- **It is difficult to keep up in the digital arms race.** Recognizing the potential risks and opportunities brought on by online organizing in the aftermath of the Arab Spring, donors have focused greater resources in recent years on digital security. With these resources, practitioners and technologists have created useful and innovative tools to protect HRDs, journalists, and other activist groups online (some of the latest were showcased in the conference, see page 16). The growing use of mobile technology around the world presents both opportunities and challenges to addressing the security needs of HRDs using smart and "dumb" phones for activism and is becoming an important component of digital security. However, implementers struggle to keep digital and mobile tools up to date and relevant in the midst of a

rapidly changing digital landscape and evolving digital attacks. In the race to keep up, many developers create tools for other developers without paying sufficient attention to user-centric design or, most importantly, the on-the-ground needs of local HRDs. As a result, local activists are overwhelmed by the complexity of online security tools and resistant to using them in their daily work, even when they are aware of the risks of using less-secure applications.

- **There is too much focus on the tools rather than the training.** Digital security practitioners recognize that there is no one-stop shop or "magic button" to make HRDs secure. Digital security tools are useless if they are not introduced with proper accompaniment and training so that trainers can assess beneficiaries' local needs, environments, and risk profiles to tailor their training and the tools they should use to meet those needs. Most importantly, trainings to introduce digital security tools are meant to help HRDs assess the level of risk they are facing and help them to think robustly about how to change their online and offline behavior and protocols to safeguard themselves, those around them, their work, and their organizations. For instance, the Hancel application[5] showcased during the conference prompts journalists to think about their emergency contacts as part of planning an assignment in a high-risk area and to create networks with colleagues and organizations that can respond in case of an attack. The contingency planning involved in using the application is just as useful as the application itself and, in fact, essential. Tools like Hancel depend on having an infrastructure of people on the ground who are able and willing to intercede when an HRD comes under attack or is in danger, and is tailored to environments where mobile technology is prevalent and where people networks are in place. Employing such a tool in environments that lack the technology and adequate "people backup" could generate a false sense of confidence. Thus, while HRDs need greater access to digital security tools and technology, it is irresponsible to disseminate tools without proper training to elevate HRDs' overall understanding of what puts them at risk and what systems and networks they should put in place to mitigate those risks. However, donors are focused on funding the latest tools, instead of "less attractive" trainings to support the responsible use of existing digital security tools and practices and efforts to localize and build the essential local support structures within civil society that these tools depend upon. Successful digital security training implies long-term engagement, but even when funding is available, it is often short-term, leaving little time for a sustainable impact.

- **A holistic understanding of security is missing.** Practitioners focused on protection strategies and assistance for HRDs and other targeted groups recognize that while recent funding efforts have centered on digital security, a more holistic approach to security is critical to overcoming HRD vulnerabilities. Activists face a range of threats that go beyond digital surveillance and attacks, including physical threats and intimidation that can also cause psycho-social harm, as well as legal and fiscal restrictions that require specialized counsel. For instance, an intrepid blogger that is adroit in encryption and other digital security tactics can easily become the target of a smear campaign if incriminating photos are published of him or her with a sensitive partner or donor, or be the victim of a physical attack if he or she does not take precautions when walking alone after meetings. Such attacks or reprisals can have significant long-term effects on an activist's well-being. Implementers are beginning to realize the importance of breaking the variety of risks down in an activist-oriented manner and providing holistic training and assistance that addresses beneficiaries' physical, digital, and psycho-social vulnerabilities and capacities. However, few trainers and resources exist that can address all of these elements cohesively. There is a minimum of knowledge that physical, digital, and psycho-social support trainers need to have about one another's work in order to effectively carry out their own work, i.e., a digital security trainer must be aware of how high stress or trauma may affect the ways in which her workshop participants will learn. Similarly, a physical security trainer should be aware of the possible consequences of an HRD carrying a smartphone at all times, even to sensitive missions or meetings, supposedly as a security measure. While digital and physical security providers are



starting to collaborate, psycho-social security remains the most underdeveloped component of protection strategies, as much less is known about these vulnerabilities and about knowledgeable experts and resources to address them. In some countries, there is also a stigma attached to receiving help for psycho-social trauma. In order to develop a holistic approach to security, implementers will need to ensure that their trainers know a minimum about each area to do their work well and ensure they are backed up by experts in the protection field, and donors will need to understand the costs and time needed to recruit talent with such a specialized skill set.

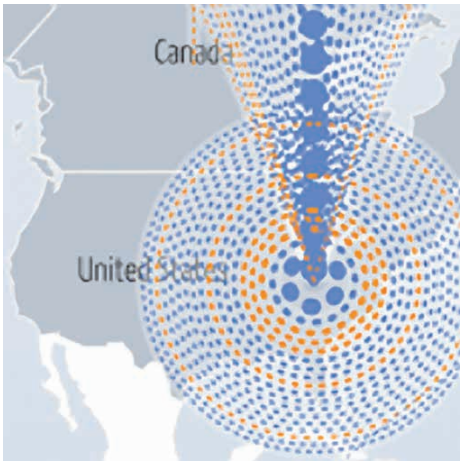
- **Collaboration is essential to get ahead of the game, but barriers make it unworkable.** Collaboration is essential if activists, implementers, and donors want to find realistic and proactive solutions to protect human rights work and those advancing these rights from sophisticated attacks by authoritarians who collaborate with each other as well. In the digital security space, technologists are familiar with the benefits of using open-sourcing, crowdsourcing, and other collaborative tactics to find innovative solutions to security challenges. As illustrated by Front Line Defenders/Tactical Technology Collective's "Security in-a-box,"[6] a collection of hands-on digital security guides tailored to the needs of a diverse range of activists, some of the best protection tools are the product of collaboration between two or more organizations. In fact, almost 100 percent of implementers surveyed after the conference indicated that they will collaborate in some form or another with other implementers. However, participants admitted that there are many barriers that make collaboration difficult and unrealistic. At the local level, egos and clan-like behavior among activists and those who support them make it difficult to get actors to rally around common objectives to make their work more secure. Many HRDs define their community in narrow terms. So, when journalists, LGBTI advocates, peasant groups, women's groups, etc., are the victims of attacks, seasoned HRDs do not assume responsibility for their safety as they do not consider these actors to be HRDs in the traditional sense. There is also widespread mistrust between activists in the Global South and the North, with activists from the South feeling mis- or under-represented and those in the North underestimating the capacity of those in the South. As a result, security tools and protocols, primarily instituted by implementers from the North, are not always informed by on-the-ground experiences of local activists. Donor procurement policies also discourage rather than encourage collaboration (i.e., by requiring a lead in consortia). Donor procurement policies are also structured around minimizing their own risks, with few donors assuming any degree of liability for the projects they fund in sensitive political environments. These policies and practices must change in order to incentivize collaboration among and between donors, implementers, and activists.

Recommendations

The following recommendations arose from the discussions.

Activists should:

- **Be proactive.** If activists are to get ahead of the game, they must be vigilant about their security. Activists must realize that using digital security tools is just one part of changing their routines in order to think ahead and put security protocols and contingency plans in place to mitigate potential threats. Activists should advocate to donors and implementers to integrate security assistance into all programming. HRDs should work with implementers and donors to establish security protocols and contingency planning as routine exercises that are integrated into their strategic planning about their work and organizations, particularly during moments of escalated violence or impending CSO restrictions that can potentially impact their operating environment. For instance, before staging protests, organizers should prepare contingency plans to address potential physical and digital attacks. Likewise, before organizing in advance of an election, groups should strategize about their response to diverse electoral scenarios and possible electoral violence. Protection International's work with The Human Rights Defenders Protection Unit (UDEFEGUA) in Guatemala, East and Horn of Africa Human Rights Defenders Project (EHAHRDP) in East and Horn of Africa, and Arus Pelangi in Indonesia can serve as examples of such an approach.
- **Wash, rinse, repeat.** Improving security management is a matter of behavioral and organizational change. The only way to ensure that security trainings have a sustainable impact on the ground is for activists to internalize and systematize what they learn in their own work and that of their organizations and then share what they learned with others. Implementing physical and digital security protocols should become second nature to HRDs as part and parcel of carrying out their daily work, as well as part of their overall efforts to maintain sustainability and resilience in the face of potential or ongoing attacks. HRDs equipped with security training should work with implementers and donors to replicate that knowledge and raise awareness about the importance of security planning among their networks and the greater public.
- **Get to the source**. Activists should work with international supporters to identify the sources of digital spyware and name and shame corporations that are providing surveillance technology to repressive regimes. They should also advocate against these practices and lobby for technology providers to revisit their policies to ensure they are not endangering activists' identities or collaborating with repressive practices in authoritarian countries. Google's "Good to Know" website,[7] which shares useful digital security tips, and its "Digital Attack Map,"[8] which illustrates Distributed Denial of Service (DDOS) attacks around the world, show a willingness by some companies to be partners in promoting digital security.



- **Go after the perpetrators.** Activists should avail themselves of international human rights mechanisms to seek legal recourse against the perpetrators of attacks. In some cases, participants shared success stories in which they were able to bring cases in international human rights institutions against their governments for perpetrating attacks against them. As the cases of Mexico and Colombia illustrate, some governments have publicly acknowledged their responsibility to protect against and prosecute attacks by state and non-state actors and are taking measures, albeit with modest results, to put protection mechanisms in place for journalists and other activists.

- **Build public support.** HRDs should avoid being isolated, smeared, and typecast by government authorities seeking to discredit them and leave them vulnerable to attacks. HRDs should seek to build domestic public support for their human rights causes by focusing on issues that matter to ordinary citizens and crafting messages that resonate with broader audiences. Conference participants shared success stories of how they turned to social media to raise domestic and international support and attention to attacks against HRDs. For instance, in Cuba, which has one of the lowest Internet penetration rates in the world, Twitter campaigns calling for the release of activists that are arbitrarily detained often lead to their release by the government, which, despite its repressive tactics, cares deeply about its international image. Some activists, such as those trained by participating organization *Videre Est Credere*, have used new technologies to build constituencies of support by exposing the public to extreme cases of bigotry and harassment through secret filming. In Mexico, Freedom House has supported films and other initiatives to increase support and empathy among average citizens in favor of the protection and survival of journalists. Conference participants also shared how they have used arts spaces effectively to engage broader audiences in human rights dialogues, as in the case of Picha Mtaani in Kenya (see photo below). By

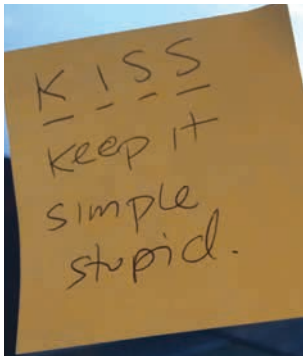
In Kenya, Picha Mtaani organized a photo exhibit to inspire reflection and dialogue among citizens, using shocking images that raised alarm around the world of the violence that plagued the country's 2007 election.

seeking an inclusive approach to promoting human rights—and tapping into social media, the arts, and other spaces to engage broader audiences—HRDs can gain widespread public support for their causes and overcome the isolation that can make them vulnerable to reprisals from governments.

- **Invest in networks and seek allies.** While collaboration is not always easy, network-building and peer-to-peer collaboration are essential elements in bolstering HRDs' self-protection strategies. While networks require significant time and trust-building, they can be very effective in allowing activists to share knowledge and protection tactics grounded in local needs and to raise the alarm and respond jointly and collectively to attacks. Networks can also be mobilized to effect change. For instance, in Mexico, Freedom House organized a working group of legislators, journalists, and human rights defenders, coined the *Grupo 73*, to successfully push through legislation to federalize crimes against freedom of expression. Activists should take a "big tent" approach to network-building and reach out to journalists and activists who share similar vulnerabilities and can serve as important allies in efforts to seek protections and raise awareness about attacks. One conference participant even illustrated how, in the face of an attack, he appealed to an intermediary with access to the government to intercede on his organization's behalf.

Implementers should:

- **Keep it simple.** Digital security training is most successful when it is kept simple at the start, focusing on basic principles, then later introducing more sophisticated layers of protection for higher-risk scenarios. If trainers, who by and large come from a technical background, share too many technical principles and tools at the onset, activists can easily get overwhelmed. Additionally, trainers should be realistic about on-ground needs and match the technology accordingly. For instance, introducing circumvention tools to activists that are operating in environments with very limited bandwidth may not be appropriate advice. Implementers and technologists should work together to simplify digital security tools and trainings to make these more user-friendly and less overwhelming for beneficiaries. Initiatives such as CommunityRED's[9] efforts to revamp existing digital security tools to make them more user-friendly— which was showcased at the conference—is a good example.



- **Focus on the training, not the tools.** Implementers should lobby donors to focus less on promoting the proliferation of new digital security tools and more on providing support for long-term training to responsibly assess which risks are run, which tools are needed, and disseminate existing tools and tactics to meet local activists' needs and improve their security habits. Implementers should also work with activists to localize existing tools to the particular cultural, technological, and political contexts they face on the ground. An example of such an effort is Tactical Tech's "Security in-a-box" toolkit for LGBT communities in the Middle East and North Africa region,[10] which was presented at the conference.

- **Promote a holistic approach to security.** Implementers are increasingly aware that HRDs and other activists are facing multifaceted threats and are in need of holistic security assistance and training to overcome physical, digital, psycho-social, and other vulnerabilities. Some steps have been taken by implementers to put together resources and trainings that take a holistic approach to security. Tactical Tech, Front Line, and others are currently engaged in a collaborative effort, still in its early stages, to establish materials, methodologies, and frameworks that engender holistic security interventions for HRDs.[11] Protection International's New Protection Manual for HRDs[12] and IREX's Securing Access to Free Expression (S.A.F.E.) initiative[13] to build regional protection hubs, featured at the conference, similarly take a holistic approach to security. Implementers must continue to focus time and effort towards promoting a holistic approach to security for HRDs, such as creating and revamping materials and curricula to address all facets of security and by recruiting trainers who can coach HRDs on self-protection strategies to overcome all vulnerabilities, including psycho-social harm. They must also stress to donors the importance of supporting more

integrated protection strategies for HRDs, including incentivizing collaboration among different implementers with expertise in physical, digital, and psycho-social security.

- **Practice what they preach.** Surprisingly, many implementers and donors that support security assistance do not have proper security protocols in place in their own operations. If implementers are serious about promoting security for HRDs, they must change and systematize their own security protocols as well. In order to do so, however, implementers need to assign a dedicated person to review and institutionalize internal security protocols, including communications, travel, and other aspects of routine work that can put implementers and their local partners in danger. They should also analyze security realities country by country and build security protocols and contingency plans according to the security profile of each country in which they operate and have local partners.

- **Get the message out.** Many participants in the conference acknowledged that they realized the seriousness of the risks they face when they or someone close to them was under attack. If the human rights community is to get ahead of the curve, implementers need to spread the message about the importance of security. In addition to carrying out threat assessments and trainings for targeted activists, implementers must seek to reach a wider audience to raise awareness among HRDs and others about the very real risks they face and to promote protection strategies as part of HRDs' overall efforts to strengthen their sustainability and resilience. One way to do so might be for implementers to collaborate on a campaign to sensitize populations and raise awareness about security globally with an aim towards changing behaviors over the long-term. An effective campaign would also need to secure buy-in from partners on the ground and from visible champions within the international community, and would be sensitive to the unique challenges and vulnerabilities faced by women HRDs.

- **Share the knowledge.** Although implementers acknowledge the danger of introducing digital security tools to activists without proper training and accompaniment, HRDs yearn for more centralized and easily accessible information about protection strategies in order to educate themselves and their networks. To address this need, implementers should encourage the creation of platforms to share common security tools, tactics, and resources and the establishment of referral networks to disseminate trusted and vetted information about security providers and emergency assistance options for local HRDs. For instance, in Mexico, Freedom House is mapping all emergency assistance providers in order to identify what kind of assistance is available and pinpoint where there is duplication or gaps. This map will allow Freedom House efforts to serve as a referral center for HRDs and journalists seeking emergency assistance throughout Mexico.

Donors should:

- **Walk the talk.** If donors are serious about security, they must also change and systematize security protocols internally so as to ensure they are not the weakest link in interactions with activists (including both online and offline interactions). Doing so would require introducing digital security protocols in what are oftentimes complex and archaic communications systems. As such, this effort would require aggressive advocacy by aid officials who are proponents of security to win buy-in from high-level government authorities. A common concern among activists in repressive environments deals with donors' transparency-related policies, which allow the public to request and scrutinize sensitive communications between donors and activists on the ground who may face reprisals for receiving foreign assistance or engaging with so-called foreign agents. Thus, walking the talk would also require donors to consult activists on "do no harm" principles, such as how best to engage them so as to avoid undermining their security. U.S. government and other donors that have more proactive policies in place to protect the identity of sensitive beneficiaries should also advocate to other donors to consider revising their transparency policies to take into account the security of beneficiaries. It may be possible to take advantage of existing Emergency Assistance Programs, such as Lifeline, Dignity for All, or others, to help coordinate among multiple donors to achieve and implement common security standards to be used by all donors in their communications with HRDs in areas of threat. Most importantly, donors must also walk the talk by elevating the importance of human rights as a fundamental

prescript for their development work. Doing so in a credible way means embedding human rights principles into all development programs, and engaging in forceful diplomatic challenges against authoritarian laws criminalizing foreign assistance. Donor agencies and foreign ministries should articulate coordinated strategies and messaging that reinforce the importance of human rights. Top officials should never shy away from espousing human rights as a core of foreign policy and development aid publicly, and in their talking points when engaging with repressive regimes.

- **Invest in security.** Donors should use funds as a tool to prioritize security, but to do so, they must also be realistic and provide assistance that recognizes the on-the-ground needs and realities of carrying out protection programming effectively. For instance, to understand local security needs, U.S. government donors should require country development officers and diplomatic desk officers to conduct risk assessments as part of the democracy, human rights and governance (DRG) assessments. Donors should coordinate among themselves to make it a common donor practice to integrate some level of appropriate security training into all relevant programming and ensure that grantees incorporate enhanced digital contracts and security elements into their agreement language. Donors should also be realistic and realize that networks are not built in a year, and that effective training requires layered relationship- and capacity-building. As such, they should invest higher levels of funding to support the recruitment of quality personnel (with higher consultant fees) that can provide a holistic approach to security. Donors should also provide multiyear funds to consolidate lessons learned and strategic planning, and allow for the long-term training and accompaniment that is necessary to effectively change behaviors and build resilience among HRDs.

- **Stress the state's responsibility to protect.** U.S. government and other foreign donors should use coordinated bilateral engagements with countries in which HRDs and other targeted populations are under attack to stress the state's responsibility to protect these populations. Donors should support existing protection mechanism models in countries such as Colombia, Mexico, and, most recently, Brazil and seek CSO input into these efforts to ensure they achieve credible results. In Mexico, U.S. assistance under the Merida Initiative was directed not only at security-sector reform but also at strengthening rule of law by bolstering the state's protection mechanism for journalists. Similarly, foreign assistance to other countries should be conditioned on, and provide support for, their implementation of measures to protect targeted populations. For instance, governments in Africa and the Middle East that are highly reliant on foreign assistance, and face similar challenges protecting targeted populations like Mexico, should be encouraged to put protection mechanisms in place and dedicate the resources and personnel to make these mechanisms effective with the help of foreign technical assistance and capacity-building. These efforts would also be in line with the recommendations of the latest Report of the UN Special Rapporteur on the situation of human rights defenders,[14] and, as such, the UN could be a potential donor in this effort. Donors should also work with judiciaries and other key institutions to tackle the root cause of HRD vulnerabilities, which is often rampant impunity.

- **Foster collaboration between government and private donors.** Representatives from USAID and other key donors, including the U.S. State Department, the United Nations, Wellspring Foundation, and others, were present and active at the conference. Yet, more efforts are needed to engage and secure buy-in from government and private donors, as well as the corporate community, to bolster protections for HRDs, recognizing the role that each sector has to play and their relative interests in protecting and advancing fundamental freedoms. In an era of austerity, pooling resources and picking priorities will be critical in efforts to encourage collaboration among government and private donors. Government and private donors should hold regular but (for security purposes) confidential donor forums to know what each donor is doing and how protection efforts can be complementary, as not enough of this is happening both within government aid agencies and ministries and between government and private donors. Multilateral donors, such as the UN, World Bank, regional development banks, and others, should be brought into conversation, particularly on how to promote complementarity, and work together to combat the growing wave of restrictions against foreign funding for HRDs and CSOs in repressive countries. U.S., Canadian, Dutch, Swedish, Norwegian, and other government

donors with more forward-leaning policies on human rights assistance should also engage in hard and honest talks with other donors about taking a more proactive stance on supporting and protecting HRDs and tackling widespread CSO restrictions, including foreign funding restrictions.

- **Incentivize collaboration among implementers.** Donors should promote collaboration among implementers, including non-profits and the private sector, to find joint and innovative solutions to the security threats that HRDs face. Donors should host private networking opportunities to bring implementers with diverse expertise and comparative advantages together so they can not only learn from one another about protection strategies but also engage in matchmaking on future collaborations. Donors should also incentivize collaboration in how they structure funding, including by providing higher levels of funding or higher thresholds for administrative costs, for proposals from consortia. Although donors prefer to concentrate their funding in well-established international CSOs, it is important that collaborative mechanisms involving the delegation of significant responsibilities and funding to local or regional CSOs be encouraged, perhaps through innovative and well-managed consortium approaches.

Reference Guide

Tools showcased at the conference:

- Google, UProxy, www.google.com/ideas/projects/uproxy/
- Tactical Technology Collective, Tools and tactics for the LGBT community in the Arabic region, https://securityinabox.org/en/context/01
- Civil Rights Defenders, Natalia Project, http://natalia.civilrightsdefenders.org/
- IREX, S.A.F.E. Initiative, http://www.irex.org/project/safe-securing-access-free-expression
- NDI, Level Up, www.ndi.org/democracy-and-technology
- CommunityRED, Simplifying Digital Security Apps, www.communityred.org/
- Videre Est Credere, Safe and Secret Recording of Abuses, www.videreonline.org/
- Freedom House/International Center for Journalists, Crowdsourced Map of Attacks against Journalists, https://periodistasenriesgo.crowdmap.com/
- Factual, Hancel, http://hanselapp.com/indexEN.html
- Protection International, New Protection Manual for HRDs, http://protectioninternational.org/publication/neaw-protection-manual-for-human-rights-defenders-3rd-edition

Other resources available:

- Freedom House, Emergency Assistance Funds, www.freedomhouse.org/program/emergency-assistance-programs#.UvPlKfldVg0
- Freedom House/CommunityRED/Front Line Defenders/KheOps/Internews International/ISC, UVirtus, www.uvirtus.org/
- Internews International, www.internews.org
- Information Security and Capacity Project, iscproject.org, info@iscproject.org
- Tech4Net, help@tech4net.org
- Google, Good to Know, www.google.com/goodtoknow/
- Amnesty International, Panic Button, https://www.amnesty.org/en/news/amnesty-international-app-protecting-activists-technology-award-2013-05-22
- Google, Digital Attack Map, www.google.com/ideas/projects/digital-attack-map
- Tactical Tech, Security in-a-box, https://securityinabox.org/
- Front Line Defenders, Digital Security, http://frontlinedefenders.org/digital-security
- Committee to Protect Journalists, Journalist Security Guide, http://cpj.org/reports/2012/04/journalist-security-guide.php
- UN, Plan of Action on the Safety of Journalists and the Issue of Impunity, http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/safety-of-journalists/un-plan-of-action/
- Humanitarian Practice Network, Operational Security Management in Violent Environments, www.odihpn.org/index.php?option=com_k2&view=item&layout=item&id=3159

Endnotes

1 http://www.freedomhouse.org/event/what-next-quest-protect-journalists-and-human-rights-defenders-digital-world#.UtQ85_RDtyM

2 http://www.freedomhouse.org/event/what-next-quest-protect-journalists-and-human-rights-defenders-digital-world#.UtQ85_RDtyM

3 Conference discussions were held on the basis of non-attribution to any individual. The following summary reflects the work of Freedom House. The report benefited greatly from the contributions of all participants, but they do not bear responsibility for its content. It seeks to distill the key findings and recommendations and is not meant to be an exhaustive account of the discussions that took place.

4 http://www.freedomhouse.org/blog/exporting-repression#.UtQ8i_RDtyM

5 http://hanselapp.com/indexEN.html

6 https://securityinabox.org/

7 http://www.google.com/goodtoknow/

8 http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16091&view=map

9 http://www.communityred.org

10 https://securityinabox.org/en/node/3292

11 https://tacticaltech.org/holistic-security

12 http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/

13 http://www.irex.org/project/safe-securing-access-free-expression

14 http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session25/Documents/A-HRC-25-55_en.doc

Freedom House is a nonprofit, nonpartisan organization that supports democratic change, monitors freedom, and advocates for democracy and human rights.

1301 Connecticut Ave. NW., Floor 6
Washington D.C. 20036

120 Wall Street, 26th floor
New York, NY 10005

www.freedomhouse.org

202.296.5101
info@freedomhouse.org