Whispering when Everyone is Listening

Low-Tech Communications Technology Implementations in High-Risk Contexts

Keith Porcaro / Laura Walker Hudson

Introduction

Technology has the potential to disrupt existing community power structures, rewriting relationships both within a community and outside it. For communities that are particularly isolated or at risk, technology-focused projects can enable data collection, conflict mitigation, and service delivery efforts that would otherwise be impossible due to safety and other logistical concerns, and empower marginalised members of the community to participate in community dialogue and assert their needs.

Although technology can help reduce risk to community members and staff, it can also calcify negative power relationships, particularly if access to technology is limited to certain members of a community (such as male heads of households) – or restricted completely. Further, programmes using technology can create expectations of action that are incongruent with project goals or standards of beneficiary accountability. These risks can be mitigated. Community-aware approaches to programme start-up, execution, and exit can help ensure not only a programme's short-term success, but also its legacy, long after the final evaluation is complete. This article examines relevant case studies and suggests useful programme practices for high-risk implementations, from community outreach and crafting message content to implementation practices that minimise risk to staff, community members, and user data. Finally, this article will discuss defining the success and evaluating the legacy of technology projects in high-risk communities.

Community buy-in and reporting systems: does acceptance matter for technology-based projects?

Community acceptance of and participation in new systems can make or break technology programmes (see Tafere *et al*, pp. 42-44). Established interests may be suspicious of the effect of capacity-building or information leaving their community; and those with less power may risk repercussions for participating or have restricted access to technology through lack of power, freedom or resources. People may raise concerns about how the data will be used and shared (see Kaiser and Fielding, pp. 37-41). Conversely, technology can enable implementers to engineer equal participation from marginalised groups, and to hear from unexpected sources and indirect beneficiaries through open and anonymous communications channels. Striking this balance effectively is crucial for maintaining negotiated access in challenging contexts.

First interactions with the community are a critical moment for setting expectations about a project's outcomes (see Tafere *et al*, pp. 42-44). Technology systems create feedback loops: expectations of action and response that may be outside a project's remit or capability. Communities may participate based on a mistaken belief in the power of programme implementers to create change. A person taking the risk of reporting an incident may experience negative repercussions, especially if no help – or no immediate, specific help – comes as a result of the report.

Efforts to qualify the intended effect of reporting systems may not survive the first word-of-mouth relay. After the 2010 earthquake in Port-au-Prince, Haiti, a local SMS gateway was set up to feed on-the-ground reports into an online mapping platform.[90] Although it was emphasised that the service was merely informational, rather than an aid request tool, it was not clear that this distinction was meaningfully understood by those who needed help. As a result, many of the incoming messages were discarded for a lack of actionability, relevance or usable location information, and as the approach was new and little understood by traditional humanitarian actors, requests were not directly taken up by aid agencies. Over-promising or failing to accurately set expectations can damage the community and project, as users take risks or expend resources to use a technology system that fails to deliver the help expected, and cease using the technology system as a result.

In one successful project, Voix des Kivus ran an 18-month pilot to monitor local events in Sud Kivu, a province in eastern DRC. The pilot sought to test the effectiveness of obtaining actionable information via SMS from communities that were dangerous or difficult to travel to. In order to ensure higher-quality data, Voix de Kivus employed 'crowd-seeding', where community reporting was routed through pre-identified representatives, each supplied with phones and credit. Due to the sensitive nature of information that was reported, such as acts of sexual violence, it was critical to obtain community buy-in and ensure that marginalised subsets of the community would be able to report.[91]

To achieve this, Voix des Kivus physically visited the target communities to explain the project and procure community consent. Each community selected three members to report incidents via phone: one from the village's traditional leadership, one representative of women's groups, and one elected representative. This enabled villagers to report incidents through the representative they were most comfortable with, and ensured Voix des Kivus would have a reliable trained cohort of reporters. Community members using the system were assured that reporters would further obfuscate sensitive information using a code sheet, which mapped two-digit numbers to a list of events. An additional digit indicated the event's sensitivity and set the degree to which the event was shared with outside parties (see Kaiser and Fielding, pp. 37-41).[92]

The pilot's success was rooted in a deep understanding of community structures, strengths and weaknesses, and the project prioritised those while still remaining practically feasible. That two of the three reporters represented non-traditional power structures potentially built trust in, and fostered the development of, additional community leaders, while respecting existing relationships.

Practical implementation of technology-based programmes for security risk management

Implementation of technology-based programmes in high-risk areas can raise many logistical challenges, particularly when distribution of hardware is necessary. Technology systems will lessen, but not obviate the need to physically visit target communities, and additional relationship-building may be needed to ensure technology is successfully used. Moreover, communities can demonstrate an ability to compensate for local logistical failures if the perceived value of the service is high enough.

In 2011 Infoasaid supported ActionAid to improve the way they communicated with drought-affected communities in Isiolo, Kenya. Infoasaid used SMS, Interactive Voice Response (IVR) and community bulletin systems to improve responsiveness and monitoring of aid reporting, and keep communities informed with critical or educational information, processes that previously required multi-day physical trips from a central office.[93] Although ActionAid Kenya continued to conduct food distributions throughout the project, one displaced community redirected their food distributions remotely when the security situation deteriorated.

250 Nokia phones were distributed to elected relief committees (RCs), along with an equal number of solar chargers. Not all communities took to the new technology. Some stopped responding or never used the system, for uncertain reasons, and some of these were so remote that, due to security and time considerations, it became impractical to return to some communities in order to troubleshoot issues.[94] This may be part of the cost of doing business in complex technology implementations, but does speak to the importance of simplicity for the end user and field-testing equipment before deployment.

[90] Meier, P. (2012). How crisis mapping saved lives in Haiti. *National Geographic NewsWatch*. 2 July. Available from: http://newswatch.nationalgeographic.com/2012/07/02/crisis-mapping-haiti. [Accessed 2 Sept. 2014].

[91] FrontlineSMS. (2011). Data Integrity Case Study: Voix des Kivus. pp. 1-2. Available from: http://www.frontlinesms.com/wp-content/uploads/2011/08/Case-Study-Voix-des-Kivus-final.pdf. [Accessed 2 Sept. 2014].

[92] *Ibid.*

[93] Infoasaid/Actionaid Isiolo. (2012). *A Learning Review of the Pilot Communications Project*. p. 4. Available from: http://www.cdacnetwork.org/contentAsset/raw-data/0abadcd6-f55a-459e-9b0e-3bcb9051c3ba/attachedFile. [Accessed 2 Sept. 2014].

[94] *Ibid.*, pp. 13-14, p. 16, p. 34.

In this example, hardware failure may have been a contributing factor to some silences – the solar chargers suffered from a high failure rate, and were unable to deliver the current expected to charge multiple phones. However, several RCs independently adjusted, switching from selling the use of the charger to selling use of the phone itself, and not one RC requested financial assistance to use the service – an unexpected success, indicating the community realised and capitalised on the value of the phone itself. Ownership of both the technology and the drought response that the implementation supported were high. When some communities fled as the security situation in the area worsened, one RC reported their new position and requested that food distributions be diverted to the new location. Staff avoided travelling to a dangerous area, and information about security risks was spontaneously provided by the community, enabling the programme to adjust.

Good project planning involves covering as many contingencies as possible, and solutions may not always be technological. Information density and complexity, such as a wide variety of potential events to report, may present challenges that have technology-adjacent solutions (see de Palacios, pp. 51-55). In Mozambique and Zimbabwe, for instance, conservation area security workers patrolling for evidence of poaching were provided with a 52-card deck of playing cards, each of which corresponded to a different event, code, and instructions for reporting the data on a form.[95] Although there are no publicly available case studies, it's possible that security focal points could have regard to information gathered in this way to augment their understanding of the local environment. Thorough understandings of service, community, and logistical dynamics are pre-requisites not only for being able to successfully roll out a new project, but also for developing creative solutions in the face of new challenges.

Protecting people by protecting data

In complex contexts, humanitarian protection efforts that use technology often involve communicating sensitive information over insecure channels. This yields immediate and direct security risks for – and from – community members and staff. Programmes must then operate under the assumption that information and communications may be intercepted or read by hostile actors, from overbearing governments to abusive family members (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16). Technological solutions such as encryption can technically solve the problem, but raise new complexities and give the impression of having something to hide (see Byrne, b. p. 57). As with much humanitarian work in such contexts, some of these risks can be mitigated with clearly articulated organisational and programme goals and approaches, and a prior consensus about how the data collected will be handled (see Kaiser and Fielding, pp. 37-41).

In general, there are very few case studies of this type of work; those listed here are most of those that the authors are aware of. This is in part due to the nature of the work, and also to the tendency for technology projects to inadequately consider, document, or publish information relating to the impact or negative security and protection implications of data gathering and dissemination. Below, we summarise some lessons learned from colleagues and partners using technology in their work, and considerations documented in our Data Integrity Guide.[96]

National actors, particularly governments, can cause complete disruptions of technology systems at any scale, depending on the threat they perceive. Even if the project is not a direct target, sudden service interruptions can severely disrupt short-term project outcomes. Further, most low-cost technology platforms, including SMS, are inherently insecure data transmission channels. This, coupled with the state's often close relationship with ICT infrastructure companies, means that the perception and content of communications can pose a risk to staff and target communities, as the potential for messages to be intercepted cannot be discounted. Even non-state armed groups in Afghanistan and Somalia have been reported to intercept SMS traffic, a relatively simple technical operation for sophisticated actors (see Gilman, pp. 8-11; see also Byrne, a. pp. 12-16).

High-risk environments are not merely so because of threats from a central government: often, risks are local, from area militias suspicious of foreign-led projects; to community stigmatisation of HIV-positive people; to an abusive husband monitoring a spouse's phone. Discovery of messages on the phone itself can put individuals at risk, and messages to programme participants should omit personal or sensitive information. Good practice can mitigate some of these issues, particularly on the local level. Examples of

[95] Le Bel, S. *et al.* (2014). FrontlineSMS as an early warning network for human-wildlife mitigation: Lessons learned from tests conducted in Mozambique and Zimbabwe. *Electronic Journal of Information Systems in Developing Countries.* 60. p. 3. Available from: http://www.ejisdc.org/ojs2/index.php/ejisdc/article/view/1256. [Accessed 2 Sept. 2014].

[96] FrontlineSMS. (2011). *User Guide: Data Integrity.* Available from: http://www.frontlinesms.com/wp-content/uploads/2011/08/frontlinesms_userguide.pdf. [Accessed 2 Sept. 2014].

good practice are crowd-seeded reporting (that works in a more restricted way than crowd-sourcing, as pre-selected phone holders are the only ones who can send information), or redacting potentially harmful personal information from messages. Moreover, community members can be advised on good practice, such as deleting sent and received messages as they come in.

Conversely, community members and staff can manipulate project data, and may be incentivised to over- or underreport based on the outcomes expected as a result of their activity, such as receiving more aid due to exaggerated crisis reports. Multi-stakeholder verification can help detect and deter falsification or exaggeration. Even when information is verified, low participation rates can distort the aggregate data picture, especially if it is a function of lack of access to technology for certain groups, rather than lack of interest. With restricted access to communities, these groups and the precise dynamics unfolding on the ground can be hard to spot.

An emerging area of concern is the complex ethics around utilising data contributed by individuals with limited technology experience. General principles of privacy and fair dealing dictate that operators of platforms need informed consent to collect and manipulate people's data (see Kaiser and Fielding, pp. 37-41). However, explaining to someone on the far side of the digital divide precisely where their data will be hosted and treated can be impractical or impossible, making it difficult for those individuals to truly consent. This is an emerging area of work only now being explored by agencies, researchers and policy-makers. Data use should also do no harm, but there are many instances of technologists not understanding the complex risk management strategies that less empowered individuals employ and accidentally publishing or exposing compromising data, putting them at risk. To take a high-tech example, the ill-fated Google Buzz platform automatically and non-consensually exposed relationships between individuals and their contacts, including victims of intimate partner violence seeking help.[97] The unclear legal and regulatory implications of hosting and collecting different kinds of data, often across multiple jurisdictions, represent another emerging concern. Context analysis, caution and a clear understanding of the technical underpinnings of the proposed platform are critical to avoiding early and costly mistakes (see Byrne, b. pp. 56-58).

Conclusion

While technology's democratisation has enabled a new wave of low-cost data collection and information projects to take place, particularly in environments that were too risky to justify a project, it has yet to reduce the competition for participant attention that any implementation faces. There is little data on the real impact that this has on project approaches, and less on the impact that such projects have, as the combined challenges of technology use and difficult operating environments militate against good impact measurement. Like any project, attention and perceptions of value by beneficiaries must be earned, with context-sensitive planning and execution (see Kaiser and Fielding, pp. 37-41; see also Tafere *et al*, pp. 42-44). This is particularly important in high-risk areas, which have increased susceptibility to shocks, and where unexpected difficulties with technology use may derail a project before it gains momentum.

Ultimately, the success of any technology project is dependent on access to the underlying platform, and excluding people from platforms only exacerbates inequality, and thus conflict. Reasons for lack of access are many, particularly in high-risk contexts, and so multi-platform, inclusive, low-tech approaches – SMS, voice systems, community bulletins, etc.– can help give people the widest possible number of options to connect with the implementing organisation. Access to technology can be transformatively empowering for local communities. Although resources may not be available to bring every technology pilot to scale, participatory programmes can help defuse local reluctance toward technology and, anecdotally at least, can increase 'buy-in', a sense of empowerment and community acceptance of programmes. In Kibera, a slum in Nairobi, foreigners began an effort to map the slum and its attendant services, but only found lasting success when Kiberans took ownership over the mapping efforts and outcomes. In the words of one Kiberan, 'When I saw the map for the first time, I was proud. This has not been done by other people. It has been done by me.'[98]

[97] Boyd, D. (2010). Privacy, Publicity, and Visibility. Presentation at Microsoft Tech Fest. 4 March. Available from: http://www.danah.org/papers/talks/2010/TechFest2010.html. [Accessed 2 Sept. 2014].
[98] Parfitt, B. (2012). Putting yourself on the map. *Geographical*. April. Available from: http://www.geographical.co.uk/Magazine/Community_Mapping_-_Apr_12.html. [Accessed 2 Sept. 2014].

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 66 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Disclaimer

EISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'EISF' in this disclaimer shall mean the member agencies, observers and secretariat of EISF.

While EISF endeavours to ensure that the information in this document is correct, EISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, EISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. EISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

Editors

Raquel Vazquez Llorente and Imogen Wall.

The editors welcome comments and further submissions for future publications or the web-based project. If you are interested in contributing, please email eisf-research@eisf.eu. Imogen Wall can be contacted at imogenwall@hotmail.com.

Acknowledgments

The editors would like to thank Lisa Reilly, EISF Coordinator, for her input and advice, and especially for her comments on the initial drafts. We would also like to extend our gratitude to Tess Dury, for her research support at the initial stages of the project, Brian Shorten for sharing his expertise with us, and Crofton Black for his early guidance and, as always, his continuous support.

Suggested citation

Vazquez Llorente R. and Wall, I. (eds.) (2014) *Communications technology and humanitarian delivery: challenges and opportunities for security risk management*. European Interagency Security Forum (EISF).

Cover photo: Mary Kiperus, community health worker, uses a mobile phone for reporting to the local nurse. Leparua village, Isiolo County, Kenya. February, 2014. © Christian Aid/Elizabeth Dalziel.

Available at **www.eisf.eu**

Other EISF Publications

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**.

Briefing Papers

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. et al. Edited by Vazquez, R.

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – *Sp. and Fr. versions available*
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 *Fr. version available*
Glaser, M. Supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Reports

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in Humanitarian Exchange 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guides

Security Audits
September 2013 – *Sp. and Fr. versions available*
Finucane C. Edited by French, E. and Vazquez, R. (Sp. and Fr.) – EISF Secretariat

Managing The Message: Communication and Media Management in a Crisis
September 2013
Davidson, S., and French, E., EISF Secretariat (eds.)

Family First: Liaison and Support During a Crisis
February 2013 *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L.
– EISF Secretariat

Forthcoming publications

Office Opening Guide