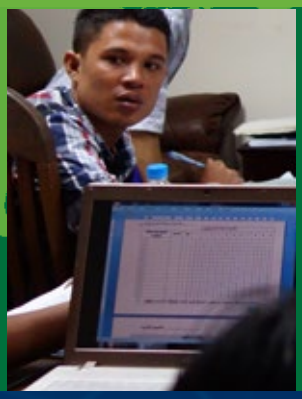
INTERNEWS CENTER FOR INNOVATION & LEARNING
innovation.internews.org

TRAINING DIGITAL SECURITY TRAINERS: A PRELIMINARY REVIEW OF METHODS, NEEDS, AND CHALLENGES

Research and writing conducted by the engine room to inform the LevelUp Project's support of digital security trainers

November 2013

the engine room

Internews

ABOUT THE ENGINE ROOM

The engine room uses research and networks to close the gaps among advocates, strategies, resources and technology. Applied research conducted by the engine room is designed to directly inform better policy and program design for the use of technology in advocacy. Engine room research prioritizes mixed methods, design and implementation processes that include the active contributions of end-users, and research outputs that are accessible and useful across the program cycle.

website: https://theengineroom.org
email: post@theengineroom.org
Twitter: @engnroom

ABOUT THE AUTHORS

Alix Dunn is creative lead and co-founder of the engine room. Alix has a background in research and training, with a focus on digital security and new media tools for social change. She has field experience in the Middle East, southern Africa, and Southeast Asia. She holds an M.A.in Media Studies from University of Oslo and a B.A. from Colorado College.

Christopher Wilson is knowledge lead and co-founder of the engine room, where he leads the design and implementation of applied research activities. Christopher has a background in human rights and research communication at the UNDP, and has worked with civil society and government actors in Latin America, Africa and Arab states to make governance data and accessible and actionable for stronger governance, transparency and accountability. He holds an M.A. in international human rights law from University of Oslo and a B.A. in Rhetoric from University of California Berkeley.

CREDITS

Design: Kirsten Ankers, Citrine Sky Design
Photos: Courtesy of Internews

CONTENTS

FORWARD

This paper comes as a global community of professional and peer trainers focused on providing digital security training continues to emerge around the world. What demarcates this community's efforts from commercial resources to help individuals and organizations stay safe and secure online is this global community's commitment to human rights defenders, activists, and media producers (bloggers, journalists, and citizen reporters)—those on the frontlines of creating, curating and disseminating critically important information. These digital security trainers' work is tailored to the rapidly changing needs of those individuals and organizations, and relies heavily on trust and respect for the unique needs and operational contexts of those they seek to support.

While the field of digital security training is not new, it has changed dramatically in recent years as access to the Internet and mobile phones increases, and as attacks on—and surveillance of—users grows in rate and sophistication. While there are also parallel efforts to improve the availability and quality of tools, services and technologies that increase the privacy, security, and anonymity of users, there is also an increased demand for professional digital security trainers who can effectively support low-resourced groups operating in complex hostile environments. There have also been concerns regarding unqualified digital security trainers emerging to meet this demand, with as potentially damaging consequences as the promotion and use of tools and services that leave users vulnerable. The goal of LevelUp, which commissioned this research, is to more effectively support the global digital security training community while coaxing out a high, shared standard for digital security trainers that is community-driven and -owned.

As this paper notes, the larger training community (and its supporters) has a wide range of next steps to move the profession forward, ranging from improved collaboration to strengthened evaluation practices to a clear standard for what constitutes a successful and sustainable training for end-users. With these forces pressuring the community to professionalize and scale effectively, the need to further identify best practices and resource gaps in the digital security support field are urgently needed. Currently, research on digital security training is almost non-existent. This paper presents methods, findings, discussion, conclusions, and recommendations for improving the growth and support of qualified digital security trainers as they seek to support the most vulnerable users around the world.

Internews is grateful to the engine room for their research and work on this paper. It is particularly important that the engine room's recommendations are for both implementation as well as further research. We are only at the beginning of understanding how to measure the challenges, best practices, and sustained impact of digital security trainings, as well as the strengths of and support needed for those who lead them.

— The LevelUp Team, Internews

1

EXECUTIVE SUMMARY

This paper draws on interviews with digital security trainers and coordinators of digital security trainings of trainers (ToT)s whose end-goal is the support of human rights defenders, civil society, activists, and local media worldwide.

The paper presents a discussion of methods and perspectives presented during interviews, and makes a number of recommendations for improving support for digital security trainers and for improving program design for ToT events. Given the lack of extant research on this topic, this paper should be read as an effort to summarize first findings, and inform the direction of future investigation and support for digital security trainers.

Among its main findings, this paper notes the following four gaps:

- A lack of sustained support for digital security trainers after they receive training at ToT events and return to their own training efforts.
- A lack of standardized frameworks for determining the effectiveness of digital security ToTs.
- A lack of standardized frameworks for trainers to conduct digital security training events around the world.
- Pedagogical approaches drawing on extensive research and developments in the field of adult education are not significantly utilized in ToTs.

Together, these shortcomings may be expected to significantly limit the potential impact of both ToTs and digital security trainings for end-users. This paper presents a set of recommendations for addressing these issues:

Recommendations

1. Promote information sharing between ToT training organizations.
2. Develop standardized metrics for assessing failure and success in digital security ToTs and end-user/local trainings.
3. Plan a dedicated and recurring event for trainers to convene and discuss methodologies and best practice globally
4. Develop training resources for ToT participants to organize their own trainings.
5. Develop and maintain an up-to-date online resource for information about evolving digital security threats and responses
6. Provide opportunities for apprenticeship, mentoring and co-training.
7. Include trainers from other fields and disciplines in digital security ToTs.

Recommendations for Further Research

1. Map, test, iterate, and monitor the ways in which ToT participants are assessed.
2. Study the work and engagement of ToT participants over time.

2 INTRODUCTION

The field of digital security capacity building is full of ideas and strong opinions about what kind of training is effective and what is not. Trainers and practitioners have their own experiences with specific approaches and outcomes, and different levels of understanding about what this implies for designing curricula for trainings and providing trainees with access to resources within the field.

In order to provide a common and objective entry point for addressing these questions, and looking towards improved practices and standards in digital security training, the engine room led a qualitative research study on the current practice of digital security training of trainers. This study was commissioned by Internews to inform its LevelUp Project.

The LevelUp initiative works to support the wider digital security training community by creating a variety of training resources and tools identified by and created in collaboration with the training community itself. This paper will inform the further implementation of Internews' LevelUp project to establish community-driven standards and resources for digital security trainers that the larger training community are invited to use, refine, and contribute to.[1]

In early 2013, the engine room conducted 10 interviews with digital security trainers and people who coordinate ToTs. These interviews were designed to surface common approaches to ToT structure and content, effective pedagogical methods in the digital security context, trends and tactics in participant selection, and effective methods for building the capacity of trainers subsequent to their participation in a ToT.

These interviews were designed to surface common approaches to ToT structure and content, effective pedagogical methods in the digital security context, trends and tactics in participant selection, and effective methods for building the capacity of trainers subsequent to their participation in a ToT.

The small number of interviews conducted is a direct reflection of how little activity there is in this nascent field of digital security trainer education, even while funding for and the number of end-user trainings continues to grow. Despite the limited number of digital security ToTs available for study, the following analysis provides important insights on how to strengthen curricula for and coordination of digital security ToTs. These findings, together with suggestions from ToT participants and coordinators, give rise to eight recommendations for enhancing the planning and implementation of digital security ToTs, and two recommendations for further research and investigation.

1 The pilot year of LevelUp runs through December 2013.

3

BACKGROUND

The digital security support field focuses on building the capacity of human rights defenders, media groups, and activists to protect themselves against digital threats. There are two primary types of digital security trainings: *end-user trainings* that focus on building the capacity of activists and human rights defenders, and *trainings of trainers (ToTs),* which are conducted with the intention of building the capacity of digital security trainers to conduct end-user trainings.

End-user trainings, which vary dramatically in scope and length, typically convene some mix of human rights defenders, activists, and media producers (bloggers, journalists, or citizen reporters) to focus on tools, tactics, and concepts that facilitate the safe use of digital resources. ToTs tend to be 5-day events designed to provide capacity development for trainers.

A considerable amount of ad hoc training-of-trainers is also conducted informally within the digital security community. Even less is known about informal digital security training, but anecdotal evidence suggests that such practices are widespread and important for building awareness and providing on-the-spot support for specific security challenges.

Hosting digital security ToTs remains relatively uncommon despite a significant uptick in recent years. Based on anecdotes and direct knowledge of the field, the authors estimate that between three and four structured digital security ToTs take place each year. Though this appears to have increased slightly over the past 12 months, due to a heightened awareness of the importance of digital security for activists. The relatively small pool of digital security experts capable of training in the human rights and development fields limits the degree to which this community can grow and respond rapidly, however. As such, this is a critical moment at which to begin uncovering evidence about strategies and outcomes of digital security ToT practices to date. The limited sample size of this study is thus both a reflection of the state of the field, and a limitation inherent in preliminary research.

Formalized trainings that do take place—both end-user trainings and ToTs—are generally funded through private philanthropic foundations and government human rights support mechanisms. The goal of funding digital security trainings (and ToTs for the trainers who lead them) is often linked explicitly to strengthening human rights and access to information. These funded efforts strive to support and protect users in repressive contexts where access to information is blocked as a result of the political motivations of government or non-state actors. Part of this includes the deployment and propagation of new or tailored technologies that are developed expressly to meet this field of challenges. Cumulatively, these efforts endeavor to support civil society, human rights defenders, activists, and journalists in their attempts to access, share and communicate information in repressive contexts without compromising themselves or their colleagues.

It is increasingly accepted that digital threats and surveillance are rapidly increasing for these communities, who require constant support and re-investment to meet complex and shifting challenges.. As a result, digital security trainings have become a common mechanism to work towards this goal. There is, however, little evidence so far indicating the conditions under which end-user digital security trainings are effective or ineffective. The authors are aware of no previous research that aims to compare the effectiveness of specific methods or training practices and that might, therefore, assist in the design of effective digital security trainings.

A significant body of literature considering the effectiveness of training efforts[2] has been cultivated within the field of media

2 See, for example, Lowell (2004) and Rouda (1995) on needs assessments; Molander (2003) and Vella (1998) on adult pedagogy, Kirkpatrick (1998) on evaluation; and Milano & Ullius (1998) on program design. For state of the art and recommendations for journalism training and support for media development, see Hume (2012 and Kaplan (2012), respectively.

development.[3] Insights from this sector should be applied with caution to the realm of digital security, however, as this literature deals consistently with professional development, wherein individuals are trained in skills and activities that they use regularly as active journalists or other media professionals. Digital security practices differ in this regard, as they are often not seen as integral to professional or ongoing activities. Indeed, the greatest challenge of digital security training is arguably normalizing safer digital security practices in participants' regular activities.

With this caveat in mind, it is nonetheless worth noting the broad consensus within literature on media development training regarding the importance of long-term engagement in training activities. This is commonly expressed as a distinction between educational and training activities that target individuals' and organizations' capacities,[4] and highlights a critical shortcoming in current digital security training models. Instruction on the *how-to* of digital security tends to dominate training events, while education on foundational concepts, practices, and technologies is both too long-term and too demanding for most training models to accommodate. There is reason to believe that some of the longer-term, more education-oriented practices described in the media development literature (e.g., in-house, on-staff trainers and sustained organizational engagement with training organizations) would dramatically enhance the capacity of end-user training participants to adapt to changing contexts and threats over time.

3 The Center for International Media Assistance defines media development as "efforts by organizations, people, and sometimes governments to develop the capacity and quality of the media sector within a specific country or region" (see http://cima.ned.org/media-development). Media development efforts often coincide with work in the areas of journalist rights and freedom of expression.

4 The distinction is described aptly in In Milano & Ullius (1998, p.4): "Education focuses on learning about; training focuses on learning how."

4

METHODS

Internews' LevelUp project selected individuals for interview on the basis of prior participation in digital security ToTs. In the planning stages it was decided that the sample should include and be divided between ToT participants and coordinators, with ten interviews conducted with former participants and three interviews conducted with ToT coordinators.

ToT coordinators are individuals in organizations that host digital security ToTs, who are responsible for designing, coordinating, leading, facilitating, and following up on ToT events. The engine room ultimately interviewed eight digital security trainers (four who had participated in formal, five-day ToT events and four who had attended shorter trainings or received one-on-one instruction, which is common in high-risk environments) and two ToT training coordinators. These individuals represented training environments in Latin America, Asia and Southeast Asia, East Africa, and Eastern Europe. ToT coordinators also had experience in North America and Western Europe. Respondents were from a wide range of professional backgrounds, including journalism, traditional civil society capacity development, web development, and academia.

This initial sample, while small, reflects the limited number of digital security ToTs conducted to date, and provides a foundation for expanding research efforts to other training activities in this area. The findings drawn from these interviews are based on respondents' experience in formal ToT events, or experiences that are analogous and applicable to structured digital security ToT processes.

Respondents were asked 15 questions grouped in four main categories, including:

- Their professional background,
- Their experiences during the training,
- Their experiences with follow-up support after the training, and
- Their digital security training work after the training.

Interview questions were open-ended, with the exception of two closed questions rating the effectiveness of pedagogical methods and the level of risk associated with a set of security threats. All answers related to training effectiveness and outcomes should be considered in the context of potential non-response bias, as this reporting could be expected to impact the perception of training organizers and funders, and consequently impact respondents' professional activities.

Interviews were recorded and transcribed prior to analysis. Interviewees were informed that interviews were recorded and that their responses would be anonymized in the report.

The answers for each respondent were coded to inform the following preliminary analyses:

- Outlining self-reported gaps and successes.
- Identifying relevant characteristics and attributes of ToT participants.
- Determining the kind of ToT or training respondents attended.
- Identifying any consequences, expanded skill sets, or changed practices attributable to the training.
- Identifying characteristics of the ideal participant for a formal ToT (or analogous informal training for trainers).

Interview and research methods used for this initial sample were designed to inform future research on digital security training metrics and processes, while providing insights to the program design of the LevelUp project.

5 FINDINGS AND DISCUSSION

The section below presents and discusses interview findings. Discussion is organized according to the following stages of a ToT's implementation:

1. assessing potential participants,
2. participant selection,
3. features of a successful trainer,
4. tool trainings,
5. live digital attacks for training,
6. effective pedagogical tactics, and
7. programming follow-up.

Assessing Potential Participants for ToTs: How to conduct an assessment?

The way in which ToT trainers assessed skill levels and backgrounds of participants before trainings varied significantly both in terms of methods and rigor. Almost all of the pre-ToT assessments focused on digital security knowledge related to tools. The majority of respondents reported that assessments were conducted during the training itself.

Participants reported the following types of assessments (in order from most frequent to least frequent):

1. Informal questions asked throughout a ToT before moving to a new module or tool.
2. Conversations during breaks whereby the ToT trainer attempted to assess knowledge.
3. Questionnaires conducted at the beginning of the training itself.
4. Questionnaires conducted before a training.
5. In-depth interview process to assess participants and determine their skill level in a month run-up to the training.

Despite the fact that almost all respondents expressed that assessments of participant knowledge were important, there was a clear lack of concrete *assessment mechanisms* and little agreement about what should be measured. The most common approach was to experiment with assessments and integrate assessments into informal conversations throughout the training (i.e. during breaks or in facilitated discussions with participants). One ToT trainer described experimenting with managing a series of interviews with potential participants before a training to get a better sense of their appropriateness before confirming that they would be invited to attend. This approach provides an opportunity for trainers to get to know their participants and to develop a heightened understanding of their backgrounds and skill sets. It also gives participants a chance to obtain and review materials before the training in order to strengthen their baseline knowledge of digital security skills and tools. Though common in other types of training, pre-assessment poses particular challenges in a digital security context, and demands a significant investment of time and energy on the part of the ToT coordinator. Nor has any attempt been made in this research to determine if pre-screening results in better quality trainers, post-ToT. A review of this tactic would be helpful to determine if it can be developed into a ToT best practice.

Participant selection: Who makes the ideal digital security ToT participant?

Choosing the right participants for a ToT is often cited as a critical point in the ToT design process, but as mentioned above, there is no standardized or widely accepted best practice for assessing participants who will attend a ToT. Because there is no standardization, tracking the kinds of participants in ToTs who are successful graduates and then reforming participant selection to identify those with a higher likelihood of success is not possible. The participant selection process described by respondents consists largely of the informal use of networks and personal contacts to identify on-the-ground actors who seem most likely to carry out trainings after the ToT. This process appears to not be institutionalized at the organizational level.

For participant selection, it is important to identify candidates who:

- will be interested in conducting digital security trainings after a ToT;
- are connected with at-risk communities and have the capacity to work with them; and
- have both the motivation and the skill set necessary to develop and maintain the knowledge they will need to become a long-term resource for such a community.

The majority of respondents noted that participant selection and pre-assessments may be easier to structure if there are clear, agreed upon variables to assess. Several helpful ways to assess participants—and the likelihood that they will be able to conduct successful training activities following a ToT—would be to examine:

- Technical knowledge (and digital security knowledge specifically).
- Level of institutionalization (Does the individual represent an organization mandated to support to other organizations and individuals? Will this translate into actual support for training activities?)
- Training and teaching experience.
- Connection with at-risk communities.
- Connection with technology communities.
- Involvement in activist, social good, social change, and advocacy work.
- Connection with the international development community.
- Language skills.
- Context of operations and activities.

These categories may provide a more structured way of developing participant selection processes and intake procedures. Given the size and nature of this sample, it is impossible to associate these features with documented success in ToTs.

Features of a successful trainer: Who makes the best trainers after a ToT?

Tracking the effectiveness of a ToT will require better understanding about how to measure the quality of trainers. It is impossible to show change over time and the results of a ToT without first collecting baseline data on a trainer's skill level and information about their effectiveness post-ToT. Currently, metrics for determining the success of a trainee after a ToT have largely been sourced from informal contact with trainees after ToTs and the number of trainings a trainee holds after being trained in a ToT. While informal assessments of trainer capacity, carried out by the ToT trainer before and after a ToT, can provide meaningful insights, they clearly lack rigor. Comparing the volume of trainings that a participant conducted before and after a ToT can also be useful, but it is difficult to weigh informal trainings of colleagues and friends against formally organized group trainings. Furthermore, the volume of trainings does not address the quality of those trainings.

Based on interviews with respondents, possible metrics for determining the success of a trainee after a ToT could include:

- How has the frequency, duration and scope of trainings carried out by the trainer changed?
- How has the trainer's digital security knowledge changed over time?
- What proportion of the trainer's work is focused on digital security training? And does the trainer self-identify as a digital security trainer?
- How active is the trainer in the larger digital security support community? And how has this changed over time?
- How effective are the end-user trainings held by the digital security trainer? (And how does this effectiveness compare before and after a ToT?)

Establishing agreed-upon metrics for determining the effectiveness of a trainee after a ToT is as essential as it is difficult. A set of measurements better able to quantify how a trainee improves (or fails to improve) after a ToT is one key missing piece of the evaluation process. If developed effectively, such measurements would inform every aspect of training design from participant selection to follow-up methodologies. The LevelUp project is uniquely placed to develop, test, and iterate indicators of success that can be used as benchmarks as well as monitoring and evaluation mechanisms for the digital security training field.

Tool training: What are the most important tools to train on at a ToT?

The most prevalent curriculum used at ToTs reviewed in this study is Security in a Box (SIAB). SIAB divides digital security training and learning around major types of data transfer and storage and makes explicit tool recommendations for understanding and mitigating digital security threats. Trainings based on SIAB often focus on training end-users to use tools. As such, ToTs that rely on SIAB as a core curriculum often involve training trainers to teach end-users to use digital security tools. It

is not possible to train on all of the tools included in SIAB in a single training (both because of the sheer number of tools and the fact that not all tools are relevant in all contexts).

In this study, respondents were asked what tools they train on most frequently. The purpose behind this was to better understand the demands placed on trainers, and to determine how to allocate time spent on tools in ToTs. The most frequently taught tools, in order of frequency, were:

1. TrueCrypt,
2. Tor,
3. Keepass,
4. portable applications ("portable apps"),
5. anti-virus software (Avast was mentioned specifically), and
6. "wiping" or secure deletion software (CCleaner was mentioned specifically).

TrueCrypt (file encryption software) was the most commonly reported tool trained by far. Tor was the second most frequently mentioned, but almost all respondents indicated that the uptake of Tor is largely dependent on context and a user's dedication to security over usability (using Tor slows down internet connectivity and is difficult to integrate fully into online browsing). Teaching Keepass (a tool for secure password storage and management) was popular and described as a great demonstration of how security tools can also increase efficiency and make digital life easier. Portable apps (applications that can be run from a USB drive) were also used quite heavily, both as an end-user security tool and as a way to facilitate hands-on trainings. Respondents indicated that portable apps serve a dual purpose in this sense: ToT participants can use them to facilitate subsequent trainings, but they are also important security tools for those who rely on public hardware or hardware belonging to others (i.e., internet cafes, office desktops, colleagues' or trainees' laptops, etc.).

All but one of the respondents mentioned that pedagogical tactics are almost entirely dependent upon context... Geographic, cultural, and professional background can greatly influence tactics that are effective.

Interviews did not reveal consistent reasons why these tools were most frequently trained (whether due to ease of use, requests by trainees, appropriateness for specific threat models, etc.), but their popularity suggests that they are useful for communicating the conceptual underpinnings of digital security—safe data storage, stronger passwords and better password management; circumvention of censorship and online anonymity; and safer use of multiple computers. While respondents found the introduction of new tools (particularly TrueCrypt) helpful and useful in training end-users, better understanding of technical concepts (broadly how the internet works, how data storage works, how targeted malware works, how mobile networks function, etc.) was considered more durable knowledge.

Effective pedagogical tactics: What are seen as the most useful ToT tactics?

Given that a ToT provides training on how to become a better trainer, it can be challenging to differentiate between pedagogical strategies work well in training participants and what methods will work well for trainers working with end-users. Only one respondent reported any formal training in pedagogy or adult learning.

The top four teaching techniques raised in interviews with respondents were:

1. acting out technical concepts,
2. role playing,
3. technology and/or tool walkthroughs, and
4. small-group brainstorming and workshops.

All but one of the respondents mentioned that pedagogical tactics are almost entirely dependent upon context, and that it is difficult to rate the tactics in a vacuum. Geographic, cultural, and professional background can greatly influence tactics that are effective. One respondent, when discussing the value of lectures, noted that educational backgrounds of participants can have a significant impact on whether a pedagogical method is effective. In some contexts, participants are more comfortable with rote explanation and lecturing. In other contexts, lectures can be ineffective ways to promote learning, in part because they are sometimes seen as too clearly dividing between "teacher" and "student."

In addition to using contextual considerations to determine the most effective pedagogical methods, two respondents

mentioned the importance of considering content. One respondent described it as follows, using TrueCrypt as an example:

> If the goal is to explain the concept of encrypted storage of data, then role playing and more interactive methods are more likely to be effective. If the goal is to get participants comfortable with using the tool then a tool walkthrough will work better. And if there is sufficient time, mixing and matching these techniques would be the most appropriate and effective.

Given the importance of context for pedagogical methods, these ratings may be more of a proxy indicator for what the respondent is most comfortable with or uses most frequently. Interestingly, no respondent mentioned common adult pedagogy methodologies when discussing the ToTs they attended.

It is also worth noting how physical and psychosocial security issues were reflected in interviews. These concepts contribute to an integrated and holistic understanding of security that includes digital, physical, and psychosocial security[5]. According to this conception, psychosocial security encompasses an individual's personal sense of security, their general emotional state, and their sense of vulnerability or insecurity. While interviews were not structured to directly address these distinctions, physical and psychosocial security concerns were noticeably absent from descriptions of training activities. When respondents did mention psychosocial security issues, they did so indirectly, using formulations such as "people get paranoid and it affects their work." No respondents reported direct training on psychosocial elements.

Digital Attacks as Pedagogical Tools: Should ToTs train participants on (or use) digital attacks?

Digital attacks are understood here as live attacks on participants' digital devices or the digital devices of others. In contexts where impressing upon trainees the importance of digital security preparedness is challenging, digital attacks on participants can be a compelling way to raise awareness. Digital attacks might include sniffing the local Wi-Fi network that participants and others are using, taking devices to see what can be discovered about a participant, or spoofing a mobile network tower to monitor participants' mobile phone use. Different live digital attacks require different degrees of technical proficiency. None of the respondents used digital attacks on their trainees, and only one respondent cited the use of a digital attack (wireless sniffing using an Android application) at a ToT.

Digital attacks might include sniffing the local Wi-Fi network that participants and others are using, taking devices to see what can be discovered about a participant, or spoofing a mobile network tower to monitor participants' mobile phone use. While digital attacks can be useful for teaching more advanced users, there is a danger of frightening and alienating end-users...

Two respondents who expanded on their thoughts about the effectiveness of digital attacks felt it was more important that such demonstrations reveal clear vulnerabilities related to the trainees' particular context than that they be carried out live (as opposed to pre-recorded as screenshots or videos).

More than one respondent recommended that trainers carefully consider the impact that certain training methods can have on the stress level of end-users. While digital attacks can be useful for teaching more advanced users, there is a danger of frightening and alienating end-users, which can have negative implications both for the effectiveness of the training and for the well-being of participants. Open dialogue about if and when to use live digital attacks is important to include in ToTs. It also presents a good opportunity to start additional discussions about how to help end-users manage other elements of their security preparedness—specifically their psychosocial security.

Program Follow-up: What are the most effective methods of follow-up?

Organizations and trainers have tried a variety of post-ToT support mechanisms to encourage participants to carry out end-user trainings after attending a ToT. These varied, including: funding support mechanisms, hosting trainings, invitations to co-train at events, and mailing lists to provide discussion threads about emerging digital security information. This last strategy was cited by many respondents as the most common and particularly helpful way to stay connected to new information, (though several also noted that they regularly read such lists but rarely contribute). A mixed approach seemed to work best.

[5] For more see, http://www.integratedsecuritymanual.org/what-is-integrated-security.

The lack of institutionalized follow-up for digital security training and ToT participants is widely recognized as a problem within the digital security training community. That said, respondents reported that the follow-up from trainers as individuals had been excellent: personal, helpful, and reliable.

Respondents who stayed in contact with their ToT trainer(s) or organization and were offered funding support to organize their own trainings were perceived to be more likely than other participants to host a significant number of end-user trainings. It is not possible to determine whether this correspondence is causal (that these mechanisms were responsible for the increased number of trainings held post-ToT) or merely evidence of correlation (that well-selected and highly motivated participants were more likely to receive support through these mechanisms). The coordinators of ToTs interviewed for this assessment stressed that any uptick in the number of trainings that a participant held after attending a ToT was significantly determined by that trainer's own ambition and workload, and difficult to attribute directly to aspects of the ToT itself. This highlights how important participant selection is in the ToT design process.

The lack of institutionalized follow-up for digital security training and ToT participants is widely recognized as a problem within the digital security training community. That said, respondents reported that the follow-up from trainers as individuals had been excellent: personal, helpful, and reliable. Two former ToT participants reported that they continue to work with other participants (both cited the use of email to continue follow-up engagement) but that this poses challenges because this kind of long-term follow-up is not funded.

Surprisingly, few of the participants interviewed said that they received support in organizing trainings or resources to help them manage the logistical processes for holding their own training. Though no respondents expressed a desire to improve their training skills, all who were asked said that a logistics checklist or other planning support would have been (or was) helpful. Useful resources may include: a checklist for training preparation, context-appropriate curricula (ideally developed by the participant during the ToT for use when designing future trainings), a reliable source for updates on digital security vulnerabilities and threats, and access to additional opportunities to build peripheral skills (in computer science, penetration testing, and event facilitation).

6

DETAILED RECOMMENDATIONS

The following recommendations are based on suggestions from respondents, trends in the respondents' answers, and contextual information (such as the dearth of empirical data on how trainings work and how their success is measured).

The organizations and groups best placed to act on these recommendations are those that play a convening function in the digital security support community. Implementation of these recommendations should be accompanied by a longer-term assessment process and additional research to document and track efficacy.

Recommendations for Implementation

1. Promote information sharing between ToT training organizations.
2. Develop standardized metrics for assessing success in digital security ToTs and end-user trainings.
3. Plan an annual event for trainers to convene and discuss methods.
4. Develop resources for ToT participants to organize their own trainings.
5. Develop and maintain an up-to-date resource for information about evolving digital security threats.
6. Provide opportunities for apprenticeship and co-training.
7. Include trainers from outside the digital security field in ToTs.

Recommendations for Further Research

8. Map, test, iterate, and monitor the ways in which ToT participants are assessed.
9. Study the work and engagement of ToT participants over time.

Recommendations for Implementation

1. Promote information sharing between ToT training organizations and trainers. Organizations that carry out digital security ToTs currently have no established mechanisms for sharing information about effective tactics and other experiences. Facilitated exchange of such information would make it easier to assess and increase effectiveness for all parties. Such exchange could be facilitated by small convenings or through open documentation. Convenings could be focused and ad hoc, or they could take advantage of the many international events that regularly draw the participation of multiple individuals and organizations active in the digital security training space.

Documentation culture, while somewhat at odds with concerns about the privacy and security of trainees, is clearly incentivized by a desire within the field for sustainable funding. This tension could be mitigated by building privacy concerns into model practices and standardized templates for open reporting, as well as common metrics for assessing the effectiveness and outcomes of training events. Donors and policymakers also have a significant role to play supporting such activities, especially by encouraging their inclusion in proposals and budgets.

2. Develop standardized metrics for assessing success in digital security ToTs and end-user trainings. Common indicators and metrics are necessary to understand and compare the effectiveness of various digital security training methodologies. A collaborative approach should be used to develop such metrics, in order to ensure that they meet the practical needs and substantive concerns of a diverse community. Metrics developed for comparing methods and trainings in aggregate should also be capable of supporting organizations' respective reporting and monitoring obligations. Metrics should address all core areas outlined in this report: participant assessment, participant selection, training methodologies, and follow-up mechanisms.

3. Plan an annual event for trainers to convene and discuss methods. A recurring forum should be developed for trainers to share information, experiences, and proven tactics. Such a

Focused convenings of this type would also present opportunities to test new tactics and tools, and to facilitate focused engagement with specific tools under development (through focus groups or collaborative work sprints).

forum would facilitate more timely and efficient dissemination of best practices, while also developing and expanding the digital security support community. It would also provide an opportunity for focused research and tool evaluation. It might also be possible to use such a forum to facilitate interface between the training community and the wider development community, to provide feedback on tools' relevance and usability in the field. Regular convenings would be an excellent opportunity to set and monitor benchmarks on how the digital community is developing in regard to training methods and engagement strategies. Focused convenings of this type would also present opportunities to test new tactics and tools, and to facilitate focused engagement with specific tools under development (through focus groups or collaborative work sprints). The small size of the digital security support community today would limit the costs of such an activity.

Some important questions raised in interviews, which would be excellent topics for LevelUp convenings include:

- Does a background in digital security or pedagogy make for stronger ToT participants, in terms of skills acquisition and effective trainings after the ToT?
- How can end-user materials like Security in a Box (SIAB) be adapted to be used as curricula in digital security trainings?
- Are live attacks (or insecurity demos) "targeting" participants in trainings useful or harmful?

4. Develop resources for participants of ToTs to organize their own trainings. While ToTs provide substantive and pedagogical resources to help participants train end-users on digital security practices, many respondents reported that these materials were not standardized. Responses indicate that actors not supported by large organizations may face logistical and administrative challenges that prevent them from conducting successful trainings. Simple resources that could alleviate these challenges include:

- checklists for administrative preparation,
- templates for funding proposals, and
- best practices for participant selection at end-user trainings.

The digital security support community should work to create resources that enable ToT participants to more easily conduct independent digital security trainings after a ToT. This may also include long-term funding of trainers that is tied to elements of quality over quantity, such as strong in-depth follow-up with end-users (rather than focusing on the sheer number of end-users trained).

5. Develop and maintain an up-to-date resource for information about evolving digital security threats. To keep former ToT participants informed and engaged with the changing landscape of threats and new mitigation tactics, a centralized, trusted source of updated information would be useful. Currently this kind of information sharing with former trainees happens on mailing lists that are maintained by trainers after a ToT. While many respondents cited this method as helpful, the large number of different mailing lists creates redundancy. Though small, siloed mailing lists may also be beneficial for community building in a particular region, they also create excess work for trainers who maintain multiple lists. All respondents cited their respective ToT coordinators as their "go-to person" for information sharing and networking following ToTs, indicating significant reliance on individual coordinators that might not be scalable or sustainable in the long run.

Potential mechanisms for keeping former participants up-to-date without relying heavily on individual trainers could include:

- Hosted, closed social networks for former participants of ToTs (using an open-source social networking mechanism like Diaspora or Crabgrass).
- A larger trainer-focused mailing list that focuses on actionable information for trainers, listings for trainer positions or paid projects, requests for help in certain regions, etc.
- A centralized website for digital security trainers.
- Other collaboratively developed repositories of information that have dedicated moderators and information useful specifically for digital security trainers.

While LevelUp may be well positioned to initiate the work required for these solutions, the outcomes must be community-owned and community-driven if they are to be sustainable, untethered from a single organization, project, or source of funds.

6. Provide opportunities for apprenticeship and co-training. ToT participants' capacity to design and manage trainings would be significantly strengthened by regular and increased involvement in training activities managed by an experienced

trainer. New trainers should be given an opportunity to test their skills in spaces where a lead trainer can provide them with feedback and where they can experiment with new tactics. When organizations are planning a digital security training, they should seize opportunities to pair new trainers with more seasoned trainers to build the new trainer's skills. It may also be advisable for co-training activities to be included in funding proposals for this purpose. While it isn't immediately clear how to coordinate such co-trainings, respondents cited working with more experienced trainers as an effective way to build skills. The digital security training community should explore ways to implement co-trainings that adequately address security and privacy concerns.

7. Include trainers from outside the digital security field in ToTs as participants. The field of digital security training is currently siloed off from other communities of technology capacity building for activists and human rights defenders. There is relatively little interaction of digital security trainers with individuals and organizations that train activists in other technology-related fields (including social media strategy, IT infrastructure, and web development), many of whom have little or no experience with digital security, and who may themselves practice poor operational security. Simultaneously, integrating digital security practices into activists' everyday workflows and strategies is one of the key objectives of many digital security trainings. Inviting non-digital security trainers to ToTs and tailoring ToTs to non-experts may be a powerful response to this trend. If well executed, such ToTs would have the double benefit of developing digital security capacities outside of the digital security community, while also positioning influential professionals to evangelize for digital security best practices and support the growth of the community.

Recommendations for further research

1. Map, test, iterate, and monitor the ways in which ToT participants are assessed. Respondents mentioned a wide range of ways to pre-assess and select ToT participants. Detailed mapping is required to better understand the state of these practices, their motivations, and outcomes. Such a mapping would also allow for a more rigorous review of assessment methodologies, testing for accuracy and usefulness. This testing could be followed by a collaborative process of experimentation, ranging from approaches using mixed-methods (interviews, focus groups, surveys) to pre-assessments at several ToTs (and potentially at end-user trainings as well). In tandem with reliable outcome metrics (see the second recommendation for further research below), this could indicate which assessment methodologies are most effective.

2. Study the work and engagement of ToT participants over time. Rigorous research is necessary to validate existing methods and demonstrate the value of both end-user and ToT digital security trainings. Respondents to this study indicated that such research would be welcome and useful in conducting their work.

The primary outcome of ToTs can be measured by the ongoing engagement and activities of participants as digital security trainers following a ToT. To measure and evaluate this over time would require a significant amount of preparatory work and research described elsewhere in these recommendations, in order to produce the necessary indicators and benchmarks.

Standardized success metrics would in turn facilitate participants' own evaluations of their training activities, and allow for comparison and process tracing across different ToTs and ToT participants.

Usable benchmarks could be developed once methods and metrics for participant assessments have been standardized. Such benchmarks could be easily established during ToTs collaboratively with participants.

Standardized success metrics would in turn facilitate participants' own evaluations of their training activities, and allow for comparison and process tracing across different ToTs and ToT participants. Noting important security concerns with regard to how such metrics were collected and maintained, a large sample with opportunities to regularly engage with ToT participants over time (potentially through one of the mechanisms listed in the first and third recommendations for implementation), might also offer insights on some of the larger questions raised in in this white paper.

The significant amount of preparation and community-driven work upon which future research will rely, means that this recommendation is likely not feasible in the short term. Steps should be taken, however (in tandem with other recommendations in this white paper), to lay the groundwork for studying participant engagement over time. Such a long-term study would illustrate comparative advantages of specific ToT tactics and shed light on other important strategic components, such as the ideal "type" of digital security ToT participant.

GLOSSARY

Digital security: Tactics and techniques for staying safe and secure from unwanted spying or digital attack online. The field is rapidly changing as digital tools themselves and ways of using them change. The conceptual underpinnings of digital security include safe data storage, stronger passwords and better password management; circumvention of censorship and online anonymity; and safer use of multiple computers.

Digital security tools: Digital support to prevent unwanted access or attack of a person or organization's information. Individual tools are too numerous to name, and not all tools are relevant in all contexts.

Digital threat: The specific potential for an individual or group to be harmed through the use of digital tools or media. This might include the unauthorized access and/or exploitation of sensitive information, such as financial, health or identity information. It might also include digital attacks intended to damage or incapacitate hardware, software or online information. Digital threats may also include offline threats that are enabled by digital activity, such as when surveillance leads to targeted violence against groups or individuals.

End-user: Individuals who use digital tools and are the intended recipients of digital security training. For the purposes of this paper, this primarily refers to human rights activists and individuals working in civil society and media.

LevelUp: Internews' project that supports the professionalization of digital security trainers through resource development, training of trainers, and community building.

SIAB: Security in a Box, a digital security curriculum developed by Tactical Technology Collective and Frontline Defenders. SIAB focuses on data transfer and storage, and tools to improve security.

ToT: Training-of-Trainers, an event intended to build the capacities of trainers in a specific field or issue area. In digital security ToTs, digital security trainers learn technical skills, pedagogical approaches, familiarize themselves with existing resources and best practices, learn how to prepare for and conduct a training event, and more.

APPENDIX: WORKS CITED

Hume, Ellen (2004). *The Media Missionaries: American Support for Journalism Excellence and Press Freedom Around the Globe.* Miami, John S. and James L. Knight Foundation. Available at http://www.ellenhume.org/articles/missionaries.pdf.

Kaplan, David E. (Eds) (2012). *Empowering Independent Media: U.S. Efforts to Foster a Free Press and an Open Internet Around the World – Second Edition.* Washington, DC, Center for International Media Assistance, 2012. Available at http://issuu.com/cima-publications/docs/cima-empowering-independent-media-2.

Kirkpatrick, D. L. (1998). *Evaluating training programs: The four levels* (2nd ed.) San Francisco: Berrett-Koehler

Lowell, W. R. (2004). *Reliability performance enhancement: Doing the right training right.* Accessed November 16, 2004. Retrieved from http://www.mt-online.com/june2000/reliability-performance-enhancement-doing-the-right-training-right

Milano, M., & Ullius, D. (1998). *Designing powerful training: The sequential iterative model.* San Francisco: Jossey-Bass

Molanda, Michael. (2003-draft version). *The ADDIE Model.* In A. Kovalchick & K. Dawson (Eds), Educational Technology: An Encyclopedia. ABC-Clio: Santa Barbara, CA. Accessed 2nd September 2008 from http://www.indiana.edu/~molpage/The%20ADDIE%20Model_Encyclo.pdf

Rouda, R., and M. Kusy. (1995) *Development of human resources–Part 2: NEEDS ASSESSMENT the first step.* Technical Association of the Pulp and Paper Industry

Vella, J., Beradineli, P., & Burrow, J. (1998). *How do they know they know?* Evaluating adult learning. San Francisco: Jossey-Bass.

ABOUT THE INTERNEWS CENTER FOR INNOVATION & LEARNING

The Internews Center for Innovation & Learning supports, captures, and shares innovative approaches to communication through a creative program of research and development worldwide. Founded in 2011, the Center seeks to strike a balance between local expertise and needs and global learning in order to develop a comprehensive approach to understanding and catalyzing information exchange.

In Internews' 30-year history of promoting independent media in more than 75 countries around the world, the last five years have arguably seen the most changes in the global media and journalism environment. Across all Internews programs, adoption of cutting-edge technology is integral to advancing the work of the journalists, bloggers, citizen reporters, scholars and others who provide a vital interpretive role for their communities. The Internews Center for Innovation & Learning deepens and enhances our capacity to link existing expertise to research that helps define, understand and monitor the critical elements of changing information ecosystems and to pilot projects that apply and test the data, platforms and digital tools to meet information needs of specific communities. This is far from a solo endeavor. A network of partners, ranging from technologists to academics to activists is critical to creating and sustaining a dynamic and iterative collaborative space for innovation.

Internews Washington, DC Office
1640 Rhode Island Ave. NW Suite 700
Washington, DC 20036 USA
+ 1 202 833 5740

Internews Administrative Headquarters
PO Box 4448
Arcata, CA 95518 USA
+1 707 826 2030

www.internews.org
E-mail: info@internews.org
Twitter: @internews
facebook.com/internews

Internews is an international non-profit organization whose mission is to empower local media worldwide to give people the news and information they need, the ability to connect and the means to make their voices heard.

Internews provides communities the resources to produce local news and information with integrity and independence. With global expertise and reach, Internews trains both media professionals and citizen journalists, introduces innovative media solutions, increases coverage of vital issues and helps establish policies needed for open access to information.

Internews programs create platforms for dialogue and enable informed debate, which bring about social and economic progress.

Internews' commitment to research and evaluation creates effective and sustainable programs, even in the most challenging environments.

Formed in 1982, Internews is a 501(c)(3) organization headquartered in California. Internews has worked in more than 75 countries, and currently has offices in Africa, Asia, Europe, the Middle East, Latin America and North America.

Internews
Center for Innovation & Learning