Digital Security Trainers' Practices and Observations

Carol Waters

Table of Contents

Acknowledgements

The author and Tactical Tech would like to acknowledge the generosity of the trainers who gave so much of their time for interviews. This research also received feedback and support from various Tactical Tech staff and associates, including Dan O' Clunaigh, Becky Faith, Andrea Figari, Maya Ganesh, Stephanie Hankey, Fieke Jansen, Becky Kazansky, Hannah Smith, Bobby Soriano, Marek Tuszynski and Chris Walker.

Introduction and Research Questions

1 Introduction

This qualitative research study explores the practices and outcomes of digital security education and training for human rights defenders (HRDs). Through a series of interviews with digital security trainers who lead trainings, Tactical Tech sought a deeper and broader sense of what trainers do, what they have observed delivering digital security trainings to human rights defenders (HRDs) for over 15 years, and how their work has evolved,[1]

Digital security training represents only a small subset of activities designed to meet an overarching goal: the safety of HRDs in their work worldwide, also known as protection for human rights defenders. The context of this work is diverse and the challenges and threats to HRDs often fluctuate faster than adequate responses can be implemented. Increasingly, the most dynamic and challenging threats have digital attributes, which makes 'digital security' ever more formidable as these emergent threats overlap with local laws, policies and the physical and psycho-social well-being of HRDs. Those committed to helping HRDs safely navigate the increasingly threatened (and collapsing) contexts in which they operate are well aware that the 'solutions' to these increasingly complicated challenges are not simple, universally applicable, nor guaranteed to work. Amongst the different types of assistance and support proffered to HRDs worldwide, many of those addressing digital safety manifest differently. A 'digital security training' led by a 'trainer' is by no means the only model, nor should it be. There are a number of approaches and models that can be explored by the digital security training community as well as local HRD communities, including forms of peer education and advocacy, self-directed learning, organisation- and network-level approaches and hybrid models best suited to individual HRDs in need. To date, there has been almost no research, development or comparisons among carefully iterated and tested learning approaches and models aside from the trial-and-error experiences of individual trainers or training organisations.

1 Please note that the research findings here do not directly represent Tactical Tech's Training Program's training philosophy, approach and methodologies as summarised in the Introduction. Similarly, the cumulative advice and opinions of the trainers interviewed represent the findings and recommendations of interview-based research and analysis; they are not prescriptive suggestions from Tactical Tech. Nor should they be read as guarantees for 'training success' from those interviewed.

One of the many findings of this study is that the digital security training community is increasingly collaborating, professionalising and exploring new approaches in a more systematic manner than before. Furthermore, there is an ever-increasing recognition of how other approaches and models of increasing HRDs' digital safety warrant exploration and support. These findings offer points of departure for further research and recommendations that are discussed in depth in the final section of this study.

2 Who This Report is For

This research is designed and intended for trainers, training organisations, intermediaries, organisations, and funders that support, commission, or lead digital security trainings for human rights defenders. On a broader level, it is also of value to anyone who includes digital security advice and training in their outreach and support of at-risk individuals and groups.

3 Research Questions

The research project within which this study was conducted was informed by questions Tactical Tech was asking about its work in digital security capacity building, including: 'How do we know that what HRDs learn in our digital security trainings helps them change their behaviour and adopt new and safer digital practices?'

The initial research question for this particular study was 'What makes an outstanding digital security trainer?' There was a belief that this question could be answered by controlling all the variables of a training apart from the trainer, enabling trainers to be clearly observed, analysed, and compared to other trainers. This question was discarded as it became clear that all the variables in trainings could not realistically be controlled for. Tactical Tech realised that trainers could not be assessed in a way that was divorced from the unique contexts that they train in and the communities they are working to support. It would also obscure the unique expertise and adaptability that distinctly *characterises* many trainers, for whom no two trainings are the same.

As such, the question 'What makes a skilled digital security trainer?' was positioned within a broader investigation on what trainers do in response to the variations across training events. What types of approaches to learning do they take? What methodologies do they use? What are the strategies they employ? A broader set of questions was then developed relating to trainers' origins, practices, methodologies, experiences, observations, and peers. Examples include:

- How did you start training?
- When you began training, did you have a mentor?
- What are three things you know now that you wish you had known when you first started training?
- What does a training need to have in order to be considered 'successful'?
- Describe the type(s) of training(s) you do now.

- How do requests/requirements from convening organisations or funders affect the quality of trainings?
- Do you do any post-training evaluations/surveys?
- How important are the following elements for trainings to be effective?
  - Participants having access local digital security expertise and resources
  - Participants having organisational/community/network support for what's being covered in a training for it to be effective in the long run
- Are you part of a community of trainers? If so, does that community have shared practices and standards?
- What distinguishes a great trainer from an average or poor trainer?

4 Common Terms and Usage

In addition to the number of common words and concepts that required baseline definitions in this research, there are several words that do not sufficiently accommodate certain key groups, ideas and concepts. In these cases, one or two words were used to keep sentences readable and to reduce the number of recurrent lists and alternative words in usage.

Any reading of this report should include 'A typology of digital security training models' in Section 3 in order to gain the basic set of definitions needed to read this study's findings.

This is perhaps unusual, but it illustrates the lack of standardisation within the broader training community, as well as the absence of research focused on this work. The different terms used by trainers to describe the capacity-building work they do when training, is itself an important finding of this research.

Types of HRD groups: The words used to describe the many types of HRD groups have been largely abridged throughout most of this study for the sake of brevity. In truth, the HRD groups trainers work with include a wide range of collectives, ranging from more formal organisations to wider movements to tighter networks of individuals. In many cases, these may be peer groups that resist a particular name or title. These are often referred to as 'organisations' and 'networks' in this study. The wide variation in these HRD collectives and connections is recognised by the authors and intended in the larger reading of the findings and recommendations below.

'Holistic' or 'Integrated' Security: The blending of digital, physical and psycho-social aspects of security may be called 'holistic' or 'integrated' security. To reflect the different phrases employed by interviewees, both are used here.

5 Factors Outside the Scope of this Study

It is crucial to note that many of the pivotal factors—frequently unknown or unclear—that affect the aspirations of digital security training-related activities for HRDs are not the objects of analysis here. Trainers are often familiar with *some* of the factors and dynamics that affect adoption of safer digital practices by HRDs. These factors can involve anything outside of the scope of what trainers observe or are involved in during the course of their work with HRDs. These independent variables represent opportune, yet challenging, areas for further research. Some of the findings from the trainer interviews in this study touch on these crucial uptake factors, but they were not the focus of this study because they often remain largely opaque to trainers.

Methodology and Participants

This qualitative research study is based on semi-structured interviews with trainers that took place over seven months in 2014 and early 2015. Interviewees were selected using snowball sampling, with an initial list based on the professional networks of both Tactical Tech and the primary researcher (through her work launching LevelUp[2], an initiative supporting the global digital security training community). Approximately 60 trainers were contacted with a request for an interview. Of those 60 potential interviewees, approximately half responded and 23 individuals were then interviewed. Fifteen interviews were conducted remotely and eight were conducted in person. Most interviews took place over an hour and half, and the researcher took detailed notes. The notes were then coded for analysis.[3]

Owing to time and funding constraints, it was not possible to compare trainers' self-reported statements and observations with those who benefited from their training, which would be a valuable area for future research. Similarly, Tactical Tech also considered assessing training evaluations from participants, post-training assessments and interviews with trainers and interviews with previous trainees, but this was curtailed due to the unavailability or inaccessibility of training documentation, including pre- and post-training assessments. While the need to conceal identifying details about participants and trainings is partly responsible for this lack of documentation, efforts should be made in the future to collect, anonymise, aggregate and organise the information required for this sort of research and analysis. Otherwise there is no material with which to observe areas of success and improvement internally.

Given Tactical Tech's role in the larger training community as an implementer and intermediary, it enjoys deep and complex ties throughout the training community. Because of this, it was felt crucial that all interviews be anonymised, which encouraged interviewees to speak freely. Additionally, since the work trainers do is sensitive and can put those they work with at increased levels of risk, great care was (and will continue to be) taken to ensure that their identities and unique voices aren't recognisable in any published research. This was in keeping with a 'Do No Harm' ethical framework.[4] Finally, because of the dearth of research in

2 See: http://www.level-up.cc
3 The amount of resulting data for analysis is considerable; it is important to note that not all of the interview material is covered here.
4 The team aimed to set standards which met those required in humanitarian and human rights documentation work.

this area, and in the spirit of the recent rise of collaboration and community building amongst trainers, Tactical Tech promised interviewees to make its research findings available to the broader training community.

1 Research Context

This research should be understood against the backdrop of recent trends focused on improving existing approaches to digital security training. These initiatives have emerged for several reasons, including the rising profile of the sector, an increase in the total number of digital security trainings worldwide, and—according to the trainers interviewed—an increasing number of new, inexperienced trainers and organisations leading digital security trainings. These trends have prompted recent initiatives to improve digital security capacity-building for HRDs in a number of ways. Efforts to bring the wider digital security training community together for collaboration, coordination and professional development include the LevelUp Program at Internews (which Tactical Tech has partnered with since its inception, among other training organisations) and trainer-specific gatherings around the development and dissemination of Tactical Tech's Holistic Security curriculum. Other initiatives are expanding their capacity-building efforts to work at the level of organizations, networks, and 'collectives' of HRDs, instead of working with single HRDs alone. Examples of these initiatives focused on 'organisational security' include Tactical Tech's Holistic Security Programme, IREX's S.A.F.E. Programme for journalists at risk, Frontline Defenders' regional Digital Security Consultants, and the two Digital Integrity Fellowship programs led by Hivos and the Open Technology Fund. Despite these recent shifts in how digital security training and capacity-building is conducted, there has been little to no research evaluating the practices and processes of these activities.

2 Interviewee Profiles

Details about the trainers interviewed that can be shared without revealing too much identifying detail are summarised below. We sought a breadth of geographic representation (both of country of origin as well as of regions in which trainings were conducted) and tried to capture a range of individuals with various levels of experience, although there was a sub-prioritisation to interview the most experienced trainers in the community. There was also an attempt to interview a representative sample with regard to gender.

Because of the snowball method of choosing participants, many had existing ties to and professional experiences with Tactical Tech. In an attempt to reduce selection bias, we also sought interviewees with weak or non-existent ties to Tactical Tech and succeeded in interviewing seven of these individuals. Because Tactical Tech's training philosophies, methods and approaches may have impacted these findings in various ways, we denote in greater detail the interviewees' experiences with Tactical Tech below.

GENDER:

6 female; **17** male

YEARS OF TRAINING EXPERIENCE:

Years experience	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No. Trainers	2	3	2	4	1	0	3	2	1	2	1	1	0	0	0	1

REGIONAL BACKGROUND:

Regional Background	W Asia	SE Asia	S Asia	W Africa	E Africa	N America	S America	C America + Caribbean	N Europe	E Europe
No. Trainers	2	2	3	1	1	9	1	1	2	2

CURRENT REGION FOR CONDUCTING TRAININGS:

Regional Focus	C Asia	SE Asia	S Asia	W Africa	E Africa	S Africa	N America	S America	C America + Caribbean	N Europe	W Europe	Global
No. Trainers	1	2	1	1	2	1	8	1	1	4	4	18

LOCAL VS. INTERMEDIARY TRAINERS:

Here, **'local' trainers** are considered trainers who operate primarily in the community of which they are a part or in which they live. Geographically, this may range from a city to a country or, in certain cases, to a region.

Intermediary trainers are individuals who frequently operate in countries and regions in which they are not based or that they are not from. They typically work for organizations that are considered intermediaries, but many are also independent. Most of the trainers considered intermediary also operate globally, but some only operate in a few regions.

1. Number of interviewees who operate as intermediaries: **13**
2. Number of interviewees who operate locally: **7**
3. Number of interviewees who operate both at intermediary and local levels: **3**

TRAINERS' BACKGROUND:

The data below shows how trainers began their work in digital security training, as well as outlining their professional development and the support they received. **Trainings-of-Trainers ('ToTs')** are workshops designed to develop the skills of participants as current or future trainers. (Please see the next section 'A Typology of Digital Security Training Activities and Interventions' for more details on ToTs, including how to distinguish them from other training-related events, as well as descriptions of how the term is often misapplied.)

Many ToTs have been implemented by Tactical Tech globally as part of its training programme, but it's important to note that there are a wide variety of ToT models, especially amongst different training programmes and trainers.

For the sake of brevity, Tactical Tech has been abbreviated to 'TTC' below.

1. Became a trainer via intermediary work with HRDs:
    a) And participated in a digital security ToT that was led or co-led by TTC: **3**
    b) And participated in a digital security ToT that was not conducted by TTC: **3**
    c) Did not participate in a ToT as they were becoming digital security trainers: **4**
2. Became a trainer via direct, local work with HRDs:
    a) And participated in a digital security ToT that was led or co-led by TTC: **3**
    b) ToT (not TTC): **2**
    c) Did not participate in a ToT as they were becoming digital security trainers: **7**
    d) Unknown: **1**
3. Attended awareness-raising and/or training events before becoming trainers (may have also attended a subsequent training or ToT): 5

PROFESSIONAL DEVELOPMENT:

Interviewees who received mentoring and/or co-trained when they were first becoming trainers:

1. Mentored by experienced trainer(s), but did not co-train with other trainers: **2**
2. Mentored & co-trained: **10**
3. Were not mentored and did not co-train: **11**

RELATIONSHIP TO TACTICAL TECH'S TRAINING PROGRAMME AND PROFESSIONAL DEVELOPMENT:

1. Were TTC staff/consultants during this research project: **5**
2. Professional development included a high level of exposure and/or adoption of TTC's approach to trainings (often those who have attended a ToT by TTC, but not limited to this form of involvement with TTC): **6**

3. Are familiar with or work closely with TTC, but did not develop their approaches under TTC's mentorship or according to TTC's approaches: **6**

4. Weak collaborative or non-existent ties to TTC (who also have no professional development histories with TTC): **7**

A Typology of Digital Security Training Activities and Interventions

1 Introduction

Despite the steady increase of digital and physical security training for HRDs over the past 10-15 years, there are no standardised terms and definitions for the most common digital security training-related activities and interventions within the broader Freedom of Expression and HRD Protection communities. Many individuals and organisations regularly use 'training,' 'awareness-raising,' and 'training-of-trainers' as if these were universally understood and standardised terms. From their interviews it was clear that most trainers know that training-related activities are defined and implemented *very* differently depending on the trainers and organisations involved, as well as how each particular event is designed and represented to participants and funders. While this is persistently challenging for trainers, it is arguably even harder for conveners, HRDs and funders to navigate as the lack of standardisation leads to misconceptions about what the various types of training-related events entail and what reasonable outcomes can be expected from them.

There are many different types of activities, events and interventions involving digital security education and a wide variety of actors who lead and support these efforts in non-'trainer' roles. These range from ad hoc one-on-one support and troubleshooting for fellow HRDs, peer education and awareness-raising activities at small gatherings, to remote support and assistance for high-risk individuals in crisis (also commonly known as 'rapid response'). All of these involve helping HRDs improve their safety by addressing their digital security through a mix of digital education, introductions to tools, and a deeper understanding of what constitutes a threat in a given context.

Therefore, the training-related activity that this research focuses on—a 'training' led by 'trainers'—needed a more precise description that distinguished it from other common training-related activities ('awareness-raising', 'trainings-of-trainers', etc.). This led to the following typology of three common types of digital security training-related events (e.g. awareness-raising, trainings-of-trainers, one-on-one support, etc.). The typology is based on

the most prevalent definitions and descriptions of each activity type according to the trainers interviewed for this study.

This typology will help readers understand what each type of training-related activity entails and how they can be distinguished from one another, which is essential to navigating the findings that follow. Nevertheless, based on our interviews with trainers (and our experience at Tactical Tech), a broader range of roles and activities that go beyond the three predominant types of digital security-related events described here in this typology as an important area of future research.

2 Types of Training-Related Interventions

AWARENESS-RAISING

Awareness-raising aims to establish and expand participants' awareness of digital threats, how those threats may affect them, why they should take certain steps to reduce their risk and may also include some low-level advice on how to do this. This advice is usually limited to easy steps audiences can take to improve their security and privacy, primarily focused on changing settings in the tools and services they already use (e.g. making their Facebook accounts private instead of public) and advice on choosing certain tools and services over others (e.g. choosing email and other services that offer HTTPS/SSL encryption throughout a session instead of just on the log-in page). It's useful to think of awareness-raising as one type of 'introductory' experience or 'first exposure' as part of a larger spectrum of events and approaches with the same over-arching goal: for HRDs to have the necessary skills, knowledge and ability to use digital tools and services in an informed way to reduce risks according to their unique needs and context.

Three features of awareness-raising activities help differentiate it from 'traditional' training events. Confusing the two, or using 'training' as a synonym for awareness-raising, often leads to a number of negative outcomes, from poorly managed expectations to miscalculated program and event design, all at a cost to HRDs, conveners and funders. Awareness-raising events can be distinguished from 'traditional' training events (described in the subsequent section) by their scope, length and ratio of participants to the individual(s) leading the event, as well as the requisite skill set of those who lead them.

Scope of issues and content covered: Awareness-raising generally focuses on helping participants become aware that risks to their privacy and security exist, what those risks are in a broad sense and learn easy steps they can take to improve their security and privacy. Practical advice is primarily focused on changing settings in the tools and services they already use (e.g. making their Facebook accounts private instead of public), choosing certain tools and services over others and being more aware of the channels of communication they use for certain activities. Often participants are given handouts, guides or links to further resources to use for self-directed learning.

Awareness-raising events often include brief introductions to of privacy- and security-enhancing tools. These same tools are usually covered with more depth and hands-on usage

during trainings. But because of the complexity and poor usability of effective privacy and security tools for the majority (that also meet the requirement of being free and open source tools), most users are less likely to download and/or use these suggested tools, especially if they are unfamiliar and unused by their peer groups. If they *do* take the steps of finding, downloading and trying to use these tools, many will need assistance to successfully install and use them. Otherwise, they run the risk of becoming frustrated and possibly avoiding them in the future.

According the trainers interviewed for this study, awareness-raising events aren't designed to provide in-depth, hands-on learning or tailored assistance on intermediate and advanced approaches and tools often required to mitigate the kind of risks typically faced by HRDs. For many HRDs, this is where training, robust self-learning (which most non-technical users are less likely to effectively accomplish alone) or some form of sustained hands-on learning and support is needed or they risk becoming 'stuck':

> *If you have security awareness, you're mainly just choosing services on the Internet. After that you need to use a tool to take it to a new level. So eventually you hit a wall. An example of this would be email: you're aware that emails can be read, but your awareness gets stuck and you can't use any tools that would prevent this. So you end up asking yourself what to do, but you get stuck: do you stop using email? Some of them just stop thinking about it and stop being concerned. Others become more interested and learn tools and attend more trainings. (Trainer with more than 12 years experience)*

This is how awareness-raising exists on a spectrum of approaches and activities that overlap with training, but it's unclear how often both interventions are implemented in a coordinated, sequential way for HRD audiences (e.g. participants first attend an awareness-raising event, then attend a training). As reflected in the quote above, trainers are concerned that at-risk HRDs who have only attended awareness-raising events can end up in a difficult position if they don't have the right resources and support to advance to the next level beyond the 'low-hanging fruit' covered in awareness-raising events. Such participants are aware that they need to do more (e.g. use end-to-end encryption for email or chat), but may struggle to reach the next 'stage' of learning and application, which is where training (or its equivalents[5]) come in. If HRDs struggle to find the support they need—either in a digital security training or with one-on-one support— they may decide to stop caring about privacy and security altogether.

Length of time and ratio of participants: In terms of length, interviewees described awareness-raising events as lasting anywhere from an hour to a day, and permitting a larger number of participants per individual event leader due to the more limited, lecture-based content. In contrast, trainings are 3-5 days and have a trainer-to-participant ratio between 1:3 and 1:12 trainers per participants.

5 One of these equivalents is robust self-learning, which is where static digital security guides can play a role. But, as one interviewee observed about learning styles vis-a-vis self-directed learning: 'There are different types of learners, and manuals only benefit a certain type of learner.' And in terms of technical skills and know-how: 'There is a very select [group of] people who do learn on their own, and a training workshop wouldn't work for them. They often have a better understanding of the concepts and can read about it and just do it. Guides speak to a particular type of person/learner.'

Leading awareness-raising events: A few of the trainers interviewed specialise in awareness-raising events. One trainer described this choice as a reflection of local needs. Awareness-raising was described as the most useful type of event they could do in their local community since there was no 'security culture' in their country. Therefore, raising awareness was considered a first vital step. This is often a common role for participants within their own communities, organisations and networks as well, pointing to the need for a more diverse and nuanced set of titles beyond the binary 'trainer' and 'participant' currently used.

Others expressed a deep fondness for awareness-raising events because of the unique impact they can have:

> *That's how you get them — the awareness-raising, that's the first crack. Explaining to people how the internet works in an empowering way makes me giddy happy on the inside. Being able to have that experience with people feeds my soul. And it's equally useful for everyone. (Trainer with more than 7 years experience)*

Some interviewees described how challenging awareness-raising events could be for them personally because of their deep roots in leading trainings. One expressed admiration for those skilled in leading awareness-raising events, since 'I can't do it, I can't stop talking after one hour.' Another said they were 'still trying to get a handle on how to make good use of an hour and a half because I'm so optimised for 3-5 days.'

Three interviewees also reported they wouldn't do awareness-raising events. One of these three felt that awareness-raising events are 'rarely cost-efficient, and rarely meet the expectations that are set for them' but feel, despite their choice not to do them, 'they certainly have value'.

Awareness-raising events as distinguished from trainings: The most common characteristics that distinguish awareness-raising from trainings and trainings-of-trainers (ToTs) are the absence of hands-on instruction and usage of tools by participants, the short length of these events and a lower trainer-to-participant ratio. One trainer described hands-on work as 'the difference between awareness-raising and the next step'.

Awareness-raising content is also included in most trainings, but becomes integrated with more in-depth background and context, hands-on work with tools and tactics and learning how to assess and mitigate risks. One trainer explained trainings as being able to 'plant the seeds' in a way that enabled more effective 'critical thinking skills' that awareness-raising events couldn't be expected to offer due to the brief duration of the sessions.

Almost all interviewees had anecdotes about being asked to lead trainings that ended up being awareness-raising events and expressed varying levels of frustration with this recurrent predicament. In many cases, they would either discover that there was not enough time or resources to do the in-depth work of a training. In other situations, conveners would whittle the time and resources available down until only a brief awareness-raising event or very brief lecture was possible. In many of these situations, conveners would continue to advertise the event as a training (often in spite of trainers' objections).

Although interviewees expressed frustration with the way that conveners, organisational leaders and some funders misperceived (and misrepresented) the ability of very short events to accomplish intensive training-level outcomes, almost all agreed that awareness-raising events were crucial and valuable. Notably, however, this value was identified as being subject to a point of diminishing returns. Participants may choose to stop thinking about the issue altogether if heightened levels of awareness cannot be turned into meaningful and effective actions where they feel they are effectively improving their security.

'TRADITIONAL' OR 'END-USER' TRAININGS

Training events are an opportunity for HRDs to gain in-depth knowledge and skills that they can use to improve their safety when using digital tools and services. Trainings can be implemented as part of an ongoing learning experience for HRDs, or as 'one-off' or 'stand-alone' interventions.

Core characteristics of trainings include hands-on installation and use of tools, a low participant-to-trainer ratio and a longer period of event time to sufficiently cover content and enable hands-on practice and tool use. Some trainings may be project- or event-specific and include other types of content (e.g. social media and advocacy training, online publishing, data collection and management, etc.). Others may be holistic security trainings that also integrate aspects of physical and psycho-social security. A grey area can emerge when non-security content becomes the majority of content covered during a training, however. In these situations, the training is not considered a digital security training by most trainers, but may evolve into an awareness-raising session or focus on a specific privacy or security tool without the time to build an in-depth understanding of the wider digital security issues involved.

Length of training events: There was some variation in interviewees' description of how long a training event should be. Almost every trainer interviewed described trainings taking place over 3-5 days (which a few described as the 'boot camp' model). A small minority of trainers said that a training could be done over two days at the absolute minimum, but this was considered an inadequate length of time by most, especially with the increasing number of tools, services and issues that trainers are asked to cover during trainings. For example, one trainer observed that in the wake of the Snowden revelations, the demand to cover more advanced tools that could provide end-to-end encryption was putting more of a strain on trainers, since this required longer training times in order to continue to cover fundamental content in addition to more advanced tools.

Challenges related to duration of trainings: One of the main reasons that trainings last three or more days relates to what trainers described as a typical 'first-day scenario'. The first day is often used for participants and the trainer(s) to get a sense of each other, establish expectations and for trainers to get a more accurate sense of participants' skill levels and needs.[6] Based on this, trainers will re-design their draft agenda for the rest of the event after a full day of exposure to their participants. Therefore, the first day is critical but is often used to

6 Trainers reported that conveners and organisers frequently don't understand why the first day needs to be used in this way. This is due to a number of factors, including establishing healthy group dynamics, and managing expectations. Additionally, interviewees almost universally reported that they are unable to get an accurate enough sense of who their participants were before the start of trainings.

establish a number of elements for the training to be successful, instead of simply applying a 'one-size-fits-all' agenda.

Since it is challenging for most participants to get time away from their daily responsibilities, trainings were reported as five days at the longest, but many were shorter, despite participants wanting more time. Less than five days resulted in less content covered in a more condensed manner, which is not as conducive to learning and retention. As two trainers summarised these trade-offs:

> *The average length is three days. Optimal length is five days. If you have five days, you give people room to breathe and process. Three days is packed, so five days will give people time to breathe, process and absorb. (Trainer with more than 16 years of experience)*
>
> *Most organisations want to do three days, which changes the nature of training fundamentally. We've had to drop out the participatory nature of our trainings due to time, since we need to get knowledge across as quickly as possible. (Trainer with 8 years of experience)*

Several trainers said that having five days was rare. One expressed admiration for the fact that the Tactical Tech Training Programme in particular was able to secure five days for most of their trainings.

Experimentations with the 'boot camp' model: A few trainers described experimenting with the 3-5 day training model described above. Two trainers described conducting multiple half- or one-day trainings over long periods of time due to the local availability of participants, and strongly praised this approach for better retention, skills and investment from participants.[7] These models also arguably open up opportunities for more HRD participants, especially those that don't work for HRD organisations and are unable to get 3-5 days off work or away from their jobs unrelated to their HRD work. Therefore, the 3-5 day 'boot camp' model tends to bias towards more established or more formal HRD organisations and their staff, as opposed to volunteers and loose informal networks.

Another interviewee described an approach where participants spend half of each day in trainings, leaving the second half of the day as unscheduled, open time for participants to independently practice what they'd learned, receive one-on-one assistance from trainers and explore new content in a self-directed way. This approach is also mindful of natural learning and retention limitations by not overloading participants with too much new information each day while still having a multi-day training. This trainer aimed to have ten days available for this training structure, but admitted that this was often difficult to obtain.

Two trainers described very established two- and three-day trainings that they offered with very little variation to their local community and seemed very happy with their design and execution.

7 This matches what is known about how people learn new topics. Most people can only retain between five and nine new concepts or items in a given session that may then eventually be translated into long-term knowledge and skills with practice and reinforcement. Most training participants experience five to nine new pieces of information during one to two hours of an average multi-day training workshop. (Oaks, CA: Corwin Press. Sprenger, M. (1999). Learning and Memory: The Brain in Action. Alexandria, VA: Association for Supervision and Curriculum Development.)

Ratio of trainers to participants: As mentioned elsewhere in this study, interviewees unanimously advocated for having at least more than one trainer for events because it allowed them to provide a better learning experience for participants. The maximum ratio of trainers per participants ranged from 1:3 to 1:12 amongst interviewees. Some trainers also mentioned having technically capable 'assistants' who weren't able or willing to co-train[8] as another option to help provide one-on-one assistance while a main trainer would lead.

Content covered: The range of content covered is quite varied and extensive, unless trainers take a 'one-size-fits-all' or limited 'tools-only' approach to content. More broadly, the range of content covered includes mixes of hands-on and in-depth background including learning how the Internet works, risk analysis, operating systems, basic computer security (anti-virus, passwords), device security (including mobiles), circumvention tools (Tor, proxies) and more.

TRAININGS-OF-TRAINERS (TOTS)

Trainings-of-trainers are events that aim to develop potential future trainers' skills. ToT participants can have varying levels of skill and experience, but often have some baseline of technical knowledge with the ability to expand that in a self-directed way. Many are from local movements and communities of practice, or are simply local technically inclined individuals who may or may not have a formal IT background.

These events required far more preparation and careful design by those convening and leading them, in part because the investment and expectations are higher. This includes careful participant selection, one or more in-depth interviews and extensive pre-ToT homework assignments for participants. ToTs tend to be between five and seven days in length and include participants designing and leading their own training sessions before fellow participants and ToT facilitators in order to receive constructive feedback.

One interviewee reported not doing ToTs at all, two reported almost exclusively doing ToTs instead of other types of events, and one reported half of their events as ToTs. The rest reported regular involvement in ToTs, but at a far lower rate than trainings or awareness-raising events.

Some interviewees mentioned that because funders require projects that offered 'plausible scaling concepts,' ToTs would be nominally included in projects but implemented as trainings because they were unable to identify enough participants from a target region or community with enough skills to be part of a 'traditional' ToT. According to these same interviewees, these de facto trainings would still reported as ToTs to funders.

8 Sometimes this is because a potential 'co-trainer' isn't fluent in the language of the training, but is able to provide as-needed one-on-one support to participants during hands-on work.

What Enables Effective Trainings?

As part of our efforts to gain a sense of what trainers believed led to successful trainings with long-term impact, we asked our interviewees a series of questions about the various core elements that comprise a training, which training approaches were more effective and what differentiated novice, experienced and outstanding trainers. While still focused on stand-alone or 'one-off' trainings that are not part of a broader, comprehensive effort to support participants, the content here relates to *all* types of trainings, not just stand-alone, one-time trainings.

For readers who are unfamiliar with digital security trainings as defined in this study (hands-on trainings lasting 3 or more days), a very brief timeline of what happens during a stand-alone training is provided below.

1 The Timeline of Stand-Alone Trainings

With a few exceptions—mostly recent initiatives designed to innovate on the 'traditional' training model, taking long-term approaches and/or focusing on entire organisations—Tactical Tech and many others have tended to conduct what trainers have called 'one-off' or 'stand-alone' trainings. Although there is a wide variation in approaches to implementing trainings, the following gives a brief overview of the typical timeline of most trainings:

'Initial ask' phase: This is when a training organisation is actively funding and designing a training or when a trainer or training organisation is contacted and asked to do a training. This is the phase where trainers consider the request and decide whether or not to do a training based on certain considerations (e.g. safety, good use of time, level of expressed need, etc.).

Planning/preparation phase: This is when the trainer prepares for the training, which may or may not be done with a local partner, local organisation or intermediary convener. During this phase, the scope of the training is determined (number of days, participants, number of trainers needed, etc.), participants are selected, assessments are conducted and the first draft of an agenda is formed. The participation and roles of the trainer, local partners, conveners and funders can vary widely. This is also a very busy stage for preparing logistics,

including choosing a location for a venue, the venue itself, obtaining visas and transportation, gathering materials and equipment for the event, etc.

Training phase: This is when the actual training takes place.

Post-training phase: This is when participants return to their daily lives. There may be a post-training assessment or varying degrees of follow-up.

With this basic training timeline and process in mind, we've condensed trainers' opinions and observations on the elements that result in more effective trainings.

2 Elements of a Successful Training Event

Based on experience and direct observations, the trainers strongly believe that certain elements are more conducive to an effective training, and other elements or practices impede learning or render events less cost-effective. Most interviewees iterated that the real work begins after a training ends, so the value of these recommendations extends beyond the end of an event the same way the learning and practices of participants do. Below is a summary of the top-level recommendations from the trainers interviewed for this portion of the research.

PARTICIPANTS

Having appropriate participants was repeatedly cited as being the most decisive variable for successful trainings. Not having the 'right' participants was constantly described as the reason for bad or failed trainings.

During the 'initial ask' phase (when the decision to lead or hold a training is still to be made), as well as the planning/preparation phase, trainers are often in deep negotiation with organisers and participants' organisations about who will attend the training. The 'right' participants were described as:

Being at-risk or working with those at-risk: Otherwise, their presence isn't a cost-effective proposition, as they tend to be unmotivated and bored.

Genuinely interested and motivated to learn: One trainer described asking participants to describe what they'd like to learn on a survey; if they leave this blank, this discounts them as potential participants. Another said participants asking about money or 'certifications' from the training was a red flag.

Having a similar level of skill amongst participants, irrelevant of whether they are advanced or newer to digital security: The common consensus among trainers was that widely divergent skill sets amongst all the participants was one of the biggest hurdles for an efficient and effective training. While some amount of this can be manageable, when trainers and conveners don't work together to assess participants' skill levels during trainee selection, the entire training is affected at the cost of participants, especially if there is only one trainer leading it:

> *There's a LOT of bad trainings due to participants of different levels, so as you finish each topic you're losing half the room because they can't keep up, but you have to keep up with other half of the room. If you don't pick the participants, that's what happens.*
>
> *When I started, I didn't know how minimal or little actual thought and consideration goes into trainee selection. It's about crossing T's and dotting I's [by those supporting the training]. Rarely is there any energy put into 'how can we make this training the best training event possible for the organisations and participants involved.*

AGENDA

Developing a well-crafted agenda tailored to participants is considered imperative for trainers. Having in-depth knowledge of the local and/or participants' context was mentioned as ideal, but most trainers observed that they were so often 'dropped' into trainings at the last moment that this was not always possible.

Even if they are able to prepare ahead of time with strong awareness of participants' context and needs, trainers unanimously claimed that they never 'actually know' what the participants' skills and needs are until the first day of the training, often due to incomplete information provided by an intermediary, incomplete or inaccurate self-assessments from participants or because some relevant issues only emerge during a training context. Since trainers often get a more comprehensive sense of how a training will go once a training's started, it's customary to make adjustments to the draft agenda based on the first full day or half day of the training. Therefore, initially developing a well-structured draft agenda then adjusting it in the first days of a training was described as a hallmark of a skilled trainer. Additional best agenda practices included:

- **Quality over quantity:** If trainers felt that participants needed to spend an entire day on passwords, they felt this was a better use of time than not covering anything well and wasting time on more advanced tools and concepts which participants would not be able to grasp.

- **Match the tools to the participants:** If a tool didn't work in a certain environment, or could be considered dangerous or illegal (in the case of encryption technologies). (Read more about this from the point-of-view of participants in 'Security in Context'.)

TIME

The right amount of time directly relates to the agenda. Because of common misperceptions of what digital security is or what a training entails, it's common for convening organisations to make requests of trainers that aren't possible to meet. Part of what a trainer does is work with a convener to establish a reasonable amount of time to cover a reasonable amount of content per the participants and their needs.

Environment

Although discussed less than other elements in this section, several trainers described the importance of a safe, comfortable venue. They described the need to create a 'safe space' for participants, which is a mix of creating a supportive, non-critical environment as well as a physically safe space. Being able to trust the trainer and fellow participants was a crucial part of this, without it "you might as well not have the training'"

Preparation

A majority of the trainers, especially the most experienced interviewees, identified preparation as key. Trainers described the concept of 'minimal viable preparation time' as a concept they had internalised deeply. Time was needed to properly select and assess participants, choose a venue and manage logistics, conduct contextual and technical research, as well as prepare the participants as much as possible. Without this 'minimally viable prep,' trainings ran the risk of being poor uses of time and funding.

Unfortunately, trainers are often contacted shortly before trainings begin, leaving little or no time for adequate preparation. Trainers described how this was often due to conveners throwing trainings together at the last minute to 'check a box' to meet grant requirements, or due to poor planning in general.

Ratio of trainers to participants

On average, interviewees felt that the ratio of trainers to participants for hands-on trainings should be one trainer for every eight participants. A few felt that you could go as high as one trainer for every twelve participants, but it would be at the cost of quality for the participants and would drastically limit what a trainer could cover during the event. Ultimately, interviewees described how too many participants per trainer resulted in less effective and inferior learning experiences. In some cases, a poor trainer-to-participant ratio forced trainers to turn nominal trainings into lighter awareness-raising events, since they lacked the necessary staff for an in-depth, hands-on training.

Trainings may initially be designed for more than eight participants, warranting the addition of one or more trainers to operate as co-trainers. Or the number of participants increases beyond initial estimates and a second trainer should be appointed. How co-trainers operate can vary widely; some trainers may take turns leading sessions, with their co-trainer helping individual participants who required additional assistance, or trainers could lead sessions in which they were particularly expert. Co-trainers may operate as equals from their initial involvement in a given training, or one trainer may be the 'lead.'

Aside from the recommended ratio of participants per trainer, interviewees across the board were firmly in favour of co-training whenever possible. Trainers described how working with co-trainers resulted in better experiences for participants: trainings run more smoothly and participants enjoy valuable one-on-one support that solo trainers can usually only provide at the cost of the entire cohort. Co-training lets trainers balance each others' strengths and

weaknesses, prevented trainers from feeling drained during and after a multi-day training and enabled trainers to take a rare opportunity to learn from each other. Several trainers said finding local trainers as co-trainers is ideal, but could be risky if unknown local co-trainers ended up being poorly qualified or unwilling to actually train.

Throughout the interviews, trainers expressed a strong preference for co-training in pairs or more, regardless of the number of participants, due to the benefits for participants, conveners and trainers. Despite these perceived benefits, they acknowledged that funders and/or conveners generally don't want to support second trainers out of a desire to maximise their cost-savings. This cost saving usually takes the form of requesting a training for as short a period of time as possible covering as many topics as possible while requiring the minimum amount of trainers and staff. Trainers often have to negotiate a proposed training into a feasible event by adjusting one of these three elements (content covered, number of participants or number of trainers).

If co-training is not an option, trainers described seeking out a local IT expert or individual that acted as the go-to tech support as their training assistant. They described wanting to evaluate this assistant's skills before a training. Finally, in the absence of a co-trainer or training assistant with more advanced technical skills, some trainers appreciated having an individual who was engaged, present and supportive throughout the workshop to help it run smoothly as well as gather informal feedback from participants throughout the event.

FOLLOW-UP

Trainers are keenly aware of how knowledge, adoption and successful implementation are fragile, making sustained support after trainings crucial. But despite this reality, trainers described how post-training follow-up for one-off trainings is almost never funded, even though most participants return to environments that are either unsupportive of improving digital security, and/or lack local expertise which can help participants implement what they've learned on an individual level.

This is immensely frustrating for trainers who often volunteer to help answer participants' questions via email without compensation in addition to their daily jobs. Trainers are rarely in their line of work for the pay and are happy to do work they are committed to, but for trainers who have worked with dozens or even hundreds of participants who may email requesting support, this can end up as a burden that ultimately contributes to burn-out. However, trainers know that their volunteered time spent responding to past training participants' questions via email is not the same as structured follow-up. Since training success largely hinges on participants putting what they've learned into practice, what happens in the weeks and months after a training takes place is arguably as critical as the training event itself. Therefore, trainers believe that without sustained follow-up, the success of one-off trainings is less than it could be, but they are unsure of how much this reduces overall impact. Furthermore, because of the difficulties of successfully evaluating one-off trainings without supported follow-up (discussed in greater depth in the next section), and without the funds to systematically pilot and document the comparative impact of providing post-training follow-up, it's unclear how much funded follow-up would improve the current impact of trainings. This is one of several areas worth further investigation if the sector is to better understand how trainings work.

After trainings end, motivated, at-risk HRDs return to their busy daily lives and quite understandably often don't use what they've learned in the absence of systematic support and reinforcement. Such support can come in different forms—systematic follow-up from trainers, and/or organisational reinforcement and assistance—but too often, HRDs have neither.

3 Approaches and Strategies for Effective Trainings

Trainers' descriptions of recommended teaching approaches and methods were one of the richest areas of discussion; this is a detailed summary of what they shared.

Understanding and applying Adult Learning Principles (Andragogy)

Although the method and practice of teaching is generally referred to as *pedagogy*, the wider digital security training community recently became more broadly exposed to adult learning theory, also known as *andragogy* to reflect its focus on adults instead of children. When asked about recommended training approaches and techniques for this study, adult learning was the most commonly favoured approach named by trainers. Despite relatively recent exposure to adult learning in the sector, many trainers had already learned many adult learning principles through experience, but had simply not been introduced to the body of academic theory and guidance. Most trainers interviewed said they'd been exposed to adult learning fundamentals through one of the recent initiatives working to bring the global digital security training community together to share knowledge and experience, LevelUp (initiated in 2013 at Internews, Tactical Tech played a key supporting role from its inception.)

Since adult learning fundamentals are so central to what trainers described as best practices, the following is a highly abridged version of Malcolm S. Knowles' adult education principles from LevelUp:[9]

- Adults learn best when they take responsibility for their own learning.
- Adults need to understand and accept the reason for learning a specific skill.
- Experience (including error) provides the basis for learning activities.
- Adults need to be involved in both the planning and evaluation of their learning.
- Adult learning is problem-centred rather than content-orientated.
- Most adults are interested in learning what has immediate relevance to their professional and social lives.

As will be discussed in this section, the dissemination of Knowles' work has made a significant impact on digital security trainers' approaches to trainings, with adult learning becoming a core tenet for the community, including Tactical Tech. As many trainers reported, "[It] has completely changed my method of training. I did things that I'd never do now".

9 See: https://www.level-up.cc/resources-for-trainers/pedagogical-resources/adult-learners

TAILORING TRAININGS TO PARTICIPANTS

An oft-repeated phrase used by interviewees was 'one size does not fit all'. One trainer described the challenge of improving one's skills while constantly adapting to new training contexts and participants':

> *What works in one training won't work in another context, so you will try to get your successes documented and internalised and articulated, but need to recognise that you can try it again in another context and must understand that it may not work. I gather lessons in my head about strategies about what works, but recognize but that I don't necessarily need to use those same things because they may not work. (Trainer with more than 15 years experience)*

The adoption of adult learning principles by trainers has paralleled increased explorations of how trainers can effectively integrate risk assessment or 'threat modeling' into trainings, which helps participants learn what their risks, threats and vulnerabilities are, how to identify them and then be able to design mitigation strategies for their specific needs and context.

This is at the heart of tailoring digital security trainings to individuals and distinct communities of practice in a participant-driven way. It is a shift away from a lecture-based, top-down, one-size-fits-all, tool-centric model of training, which has been a standard for much of the training community for over a decade.

One of the most experienced trainers observed that a lot of time was wasted while trainers learned what worked through trial-and-error on the job instead of learning it from well-established and pre-existing areas of the teaching profession or via structured research and testing by trainers:

> *I wish there was something planned for the industry that this became to design trainings strictly on the basis of learning from participants' impressions and feedback, and from being able to gauge what is successful in what we do and what isn't. I think if we had that from the start, we could have helped the new trainers and ourselves more quickly, because the good trainers become good via trial and error and that wastes a lot of time. And if we had a better worked out mechanism [for this, we] would have save funders a lot of time. (Trainer with more than 12 years experience)*

BUILDING AND STRENGTHENING COMMUNITIES AND NETWORKS

One of the most valuable outcomes of trainings are the human connections and community-building that emerges at trainings, which several trainers described as equally valuable to the content covered. This 'shared experience' can help 'bring solidarity' to previously unconnected or weakly connected networks, which strengthens their ability to meet their common goals:

> *Social things happen in movements, and the more connections are created within them, the stronger these movements become. What happens outside of training sessions is almost as important as what happens inside when building those connections. And this is valuable for all the other goals of these organisations.*

This is also a metric for a particularly successful event for many trainers, especially those who don't just see the training as an exchange of knowledge, but as a larger attempt to build capacity in movements working to meet a larger set of goals.

> *Successful trainings have an element where participants have a shared and common experience, and this is often more sustained than whatever was taught. This is a very human thing. In a classroom training, I don't just worry about teaching lessons. It's also about creating a safe space and time that they may never have again, and help them value that so they don't go away afterwards and never speak [about it] again.*

Because trainings and ToTs are longer, more intensive and more intimate events, this element of building networks and strengthening communities is also what can distinguish a training from an awareness-raising or other type of event:

> *Building networks is really important, because as an activist this is what you rely on the most, and I don't think this happens with awareness-raising because you don't have time to get to know people.*

In turn, these stronger networks can reinforce the content-related goals of a training. Not only can participants provide encouragement and reinforcement for the practices and tools covered in the training by having a community to use them with, they can also help participants when they get stuck back home without access to local support and expertise:

> *They can use those relationships for assistance, especially when they don't have a mentor locally who can help them. …they can also put word out if they're going into a dodgy situation and have been seeing people getting arrested at protests/demonstrations who are activists or other types of actors and you can let people know where you're going to be and that can be better than letting internal people know.*

REJECTING FEAR, ENCOURAGING EMPOWERMENT

As will be discussed in greater detail in the next section, interviewees observed that trainers who are either new to training (or experienced but ill-suited to the role) tend to adopt a fear-based, top-down, tool-centric approach to digital security training, leaving participants feeling overwhelmed and disempowered. This sense of disempowerment can contribute to participants feeling that their actions would not make a difference, and that they did not have the skills to do what was needed. Understandably, this can make trainings far less effective and leave participants with a sense of hopelessness and lack of agency. As one trainer put it, when "people are cynical, training doesn't stick and fades quickly".

Several trainers, especially active members of HRD groups and movements, strongly rejected taking a 'fear-based' approach to training, advocating a need for empowerment and confidence boosting. Others more consciously supported this after being introduced to Tactical Tech's recent work on Holistic Security in particular:

> *I now have a better understanding of how to enter the conversation… especially vis-à-vis a more holistic approach where I'm entering via empowerment instead of fear. [I] used to tell people what the pitfalls are and then try to 'fill' those. I'm now trying to get people to understand their assets and what they want to do with that. [This] has made my training life much easier because it has more buy-in [from participants]. Before I was following same path of using scare tactics in a controlled environment. I had epiphanies when talking… about how the human brain works in stress situations and what we can do in trainings to 'Do No Harm' and how to get through the door in a positive way. I remember in the beginning when I wasn't like this. (Trainer with more than 7 years experience)*

Helping to nurture a sense of empowerment reinforces other valuable experiences for participants. In addition to a greater rate of adoption, it can also encourage dissemination and sharing of what they've learned amongst colleagues in a very positive way. It also helps increase the demonstration effect for HRDs (who have not attended the training) seeing colleagues using a particular tactic or tool and feeling that 'if that person can do it, I can do it too'. Empowerment also goes hand-in-hand with a sense of confidence, which in turn helps strengthen networks as well:

> *Confidence building is valuable when building networks (not formal networks, although this can be a side effect of a workshop). Just knowing that there are people who kind of know what you know and what you do and vice versa. It's connections, and embedded in this is an experiential confidence for the individuals that never get measured. I think of this in how I became an activist – I grew my confidence through events, trainings, etc. (Trainer with more than 16 years of experience)*

DAILY EVALUATIONS AND TRAINER DEBRIEFS

Conducting 'plusses and deltas' with participants at the end of every day was a valued and established assessment practice among the trainers interviewed. Trainers ask participants to share things they thought were good or particularly great that day ('pluses'), as well as anything they would suggest changing ('deltas'). These are typically shared via post-its in as anonymous a fashion as possible (given small training groups who can learn to identify each others' handwriting over the lifespan of a training event). Trainers then collect these from participants and have a debrief session with fellow trainers and/or organisers in order to review them. They then discuss how they can adjust the agenda or approach for the following day or even the entire event to accommodate requests. In order to acknowledge what participants have shared, trainers will share a general review of the plusses/deltas from the previous day, first by sharing the things participants liked, then by discussing what they would (or would not be able to) do regarding the deltas.

This helps participants be more engaged, helps them feel heard and respected by trainers and gives them a constructive means of co-creating their own day-to-day learning experiences. It also results in better trainings, as each day is calibrated to be more effective. Finally, it provides a very clear source of evaluation during the training, in contrast to the near-absence of effective long-term training evaluation data after trainings.

This also reflects how trainers have endeavoured to improve the impact of trainings as much as they are able, given the constraints and shortcomings of the dominant funded model for one-off or one-time trainings. It also enables trainers to learn in real time what they should adjust and change, instead of only getting that feedback at the end or after a training when they are unable to do anything short of keeping it in mind for future trainings.

In the case of ToTs and as part of a larger conversation about how trainers learn, two trainers mentioned how the practice of 'pluses and deltas' and open daily debriefs among trainers was invaluable for them. One shared how crucial this was for them during their first training experience:

> *They gave me feedback and we did a 'what went well, what could have gone better' thing, and a debrief at the end of every day. That was what made it work for me, getting feedback from more experienced trainers. (Trainer with 8 years of experience)*

Regarding the act of a daily debrief where trainers discuss participants' pluses/deltas as well their own pluses/deltas on the day:

> *I thought the concept was so novel and it gave me insight in to how good trainings are done—they are talked about before/after and it was learning how to learn. (Trainer with 4 years of experience)*

CREATE A SAFE SPACE

The approach of creating a safe space for learning is also part of a broader response to the top-down, lecture-dominant, fear-based model of training discussed above. Trainers discussed how creating a safe space—physically, socially, and emotionally—for participants was deeply conducive to learning. The creation of a safe space includes hosting the event in a location where participants feel safe and comfortable, having a selection of participants who can trust each other (as well as the trainers) and "creating a social environment where people can talk about fears without feeling stupid or dumb".

USE (IN)SECURITY DEMONSTRATIONS SELECTIVELY, CAREFULLY AND ETHICALLY

Several interviewees described how their positions on 'security' or 'insecurity demos' had changed over time as they moved away from the 'fear-based, tool-centric' model of trainings. Live security (or '(in)security') demos are when trainers demonstrate how a specific type of digital attack is carried out (e.g. capturing passwords as someone logs into an online account, or directly accessing data on a laptop or mobile phone without a password). Trainers have been known to target participants without warning or permission during these demos which can

result in participants' passwords being captured and revealed to a group of participants, or having their laptop accessed while they are out of the room for lunch or break. This can leave participants feeling attacked, embarrassed or even 'singled out', which can lead to a hostile environment and poor training outcomes. A small number of interviewees even said they would not do demonstrations, but the dominant sentiment was that they are a vital awareness-raising and teaching tool for trainers, yet must be conducted sensitively. One trainer summed up a commonly shared opinion that "insecurity demos are THE MOST effective [teaching] tactic, but they can easily go astray if you're not controlling every element carefully".

GET TO KNOW PARTICIPANTS AND THEIR CONTEXT

Trainers are often are asked to lead trainings that have been poorly conceived and executed and without adequate notice. These tend not to be effective trainings because best practices for preparation—which includes the trainer's input—are no longer possible.

But when circumstances allow for a training to be put together in collaboration with trainers with sufficient lead time, trainers advocate not only carefully selecting participants, but also getting to know them and their context as much as possible if they are not from the local or larger peer community themselves. For experienced trainers, the first short notice scenario may still result in a poor training, but they tend to have a stronger 'ability to kind of learn about their audience quickly', a skill which also serves all trainers well even in well-prepared training events. This enables trainers to tailor their agenda and delivery as well as possible for the people in the room.

What Distinguishes 'Outstanding' Digital Security Trainers?

This section seeks to answer that which had initially been the primary question for the research: 'What makes an outstanding digital security trainer?' To answer this, as well as discover more useful details about the qualities of trainers across a wider spectrum, trainers were asked to describe what characterises the best trainers they know, average or 'good' trainers, and less effective trainers. In order to understand what makes a trainer 'outstanding', it's useful to discuss what also characterises less effective and average trainers in the eyes of their peers.

The characteristics in each of the three sections describe the traits most commonly described by the trainers interviewed for this study.

1 Less Effective Trainers

These characteristics describe trainers who may be new to training and are still learning, or those who have been training for quite a while but are simply poorly suited to training.

'Everything's about them'

This can range from novice-level experiences, such as being preoccupied with doing something accurately, rather than well, to personal characteristics that make them very poorly suited to training due to a preoccupation with themselves over participants.

They tend to 'teach to themselves'

These individuals may not have the skills (yet) to assess a group of participants and tailor content and approach to the needs and skill levels of participants. Sometimes this can come off negatively as 'nerds showing off' to participants.

However, this also applies to people who force their views and opinions on participants aggressively and inappropriately, or use the opportunity to demonstrate their knowledge or abilities without consideration for participants' learning and with as little two-way interaction with them as possible.

Minimal or inaccurate technical knowledge

These can be individuals new to training that aren't from technical or security backgrounds. It may also be people who feel a need to appear all-knowing, and 'fake it' for participants due to a personal need to be seen as skilled or to avoid appearing wrong.

They are often unable to answer questions well, cannot or will not explain 'why' for participants, nor frame the overall context or issues for participants. Interviewees also associated this characteristic with taking a 'because I said so' approach to participant questions; an inability to say that they don't know the answer to something and perhaps (dangerously) perpetuating rumours that are inaccurate or counterproductive.

They stick to what they know

These may be new trainers who are not comfortable or skilled enough yet in the classroom to be flexible, or they may have a limited repertoire of skills and tools beyond what they have prepared for. These may also be individuals who have trained often and are uninterested in changing or improving or unable to do so.

Because of this, participants may receive trainings that aren't as relevant to them or as useful in their daily lives as they could be. They may also feel like trainers don't understand what they do or what they need, especially if the trainer is covering content that is unusable or irrelevant.

Deep technical knowledge, but poor training aptitude

Sometimes these are simply new trainers with excellent digital security skills and backgrounds who are completely new to teaching and facilitation. But this category may also include individuals who will never be good trainers. Many trainers describe these individuals as the worst trainer candidates. These trainers can remain inaccessible to audiences and they may struggle to tailor the event or content to match the skills and needs of participants.

Use and rely on 'scare tactics'

These are trainers who scare participants and rely on fear in their trainings by 'freaking people out'. This can involve hacking into participants' devices and accounts without warning or permission ('security demos'), which can embarrass and shame participants in front of their peers. This usually backfires and paralyzes participants into inaction and leads to a poor learning environment.

It is important that scare tactics be distinguished from demos that are not fear-based exercises involving unauthorised access to participants' accounts and devices. Often the same

interviewees who condemned scare tactics would also praise demos implemented in a more sensitive way (also known as 'insecurity demos'), since many trainers believe that "insecurity demos are THE MOST effective [teaching] tactic, but they can easily go astray if you're not controlling every element carefully."

UNPREPARED

Trainers are either unprepared and have not been involved in preparation for the workshop because they've either agreed to a poorly conceived last-minute event, or they don't know what preparation entails. In the worst case scenario, they believe that they can easily just 'wing it' despite their inexperience.

POOR OPERATIONAL SECURITY

It is common to hear trainers bemoaning 'bad' trainers' perpetuating of technical inaccuracies or 'fear mongering' during trainings both within and outside of the training community. But perhaps the worst possible trainer characteristic is having poor operational security that negatively impacts participants. In the best-case scenarios, poor operational security harms no one, but in the worst-case scenarios it leads to arrests, raids, imprisonment, 'disappearances,' and local organisations having to suspend operations. An example from one of the interviewees illustrates this type of worst-case scenario:

> *[I] heard of another organisation that came in and gave the white western parachutist training… They had no concept of the threat environment, [and were] very arrogant. [The] resultant effect afterwards was within 1-2 days all those who did the training were rounded up and arrested. Moral is that the trainers didn't have their own security nailed down before. We had to turn our subsequent training into an evacuation training. The organisation went dead for a few months. They blew their money in the worst possible way. (Trainer with more than 8 years of experience)*

2 Good or 'Average' Trainers

Interviewees were asked to describe trainers 'in the middle' of a spectrum between poor and excellent, which could also be roughly described as 'average' or 'good.' These may be trainers who are on their way to becoming the best trainers in the larger global training community, or this is where most trainers consider themselves to be after a certain amount of experience and a sustained commitment to improving their knowledge and craft. As one interviewee put it, "Most trainers are in the middle. I'm in the middle." Another trainer described 'good' and 'average' as "a fantastic place to be, because that is still doing more good than harm …[and it's] how you get good."

The difference between 'average' and characteristics of 'excellent' or the 'best trainers they knew' are perhaps the most nuanced illustrations of what distinguishes 'outstanding' trainers. All interviewees expressed respect for these individuals' skills and the shared sense that the

best 'rock star' trainers were a very small minority points to the professionalism of those interviewed.

In general, average trainers have more experience behind them (ideally with support from a mentor or members of the local or international training community). As part of this, they are typically better at the overall process of developing, preparing and implementing trainings, which includes identifying poorly proposed trainings and knowing how to negotiate with conveners in order to avoid disasters or poor uses of time and funds. Their knowledge has generally grown in depth and breadth to varying degrees and they're more comfortable in front of a group of participants. This increased level of comfort has freed them to be more adaptable and flexible in response to participants' needs as well as common surprises and problems that arise.

Technical Knowledge and Skill

'Average' or 'good' trainers have solid knowledge and experience with the tools and concepts, although they may still be spending more time on the hands-on tools portion of the content than balancing the tools with concepts and other skills. Without a strong grasp of the technical elements, interviewees said or implied that individuals were not really qualified as trainers (or 'good' trainers). A couple of interviewees described trainers whose technical skills never reach a certain baseline as only capable of leading 'awareness-raising' events (both explicitly so or inaccurately advertising their events as actual 'trainings'). This reflects the earlier agreement among interviewees that hands-on use of tools was crucial in order for a workshop to qualify as a training.

Nascent facilitation skills

Good trainers were described as being able to interact with participants more effectively, but one of the grey areas between a 'good' trainer and an 'excellent' trainer appeared to be an ability to fully engage participants. Despite this, 'average' trainers were better at 'reading a room' as a group as well as individuals, answering questions and being more flexible in general. Another distinguishing element between 'good' and 'excellent' trainers was facilitation skills. 'Good' trainers had some or better facilitation skills in addition to being more skilled at teaching. 'Good' trainers were also more adept at organising a schedule, time management and being able to manage the unexpected and 'the chaos'.

One facilitation shortcoming of 'good' trainers was a potential tendency to over-facilitate and over-manage a group and event, without letting participants have as much of a sense of ownership. A second shortcoming distinguishing a 'good' from an 'excellent' trainer is a facilitation approach that "still relies too much on a lecture style".

Flexibility and the ability to 'meet participants where they are'

'Good' trainers were described as still not being able to fully engage their participants the way the best trainers can. Instead of approaching a training from a very inflexible and less accessible 'top-down' approach, 'good' trainers are capable of adapting their approach, agenda

and content in order to 'meet participants where they're at.' However they may still tend to be a bit mechanical in their delivery and have habit of sticking to a schedule and certain tools instead of being flexible and responsive to what a particular group of participants need based on their environment, current activities and skill sets.

3 The Best or 'Outstanding' Trainers

Finally, these are characteristics of a select minority of trainers that interviewees consider to be 'excellent', 'the best' or 'rock stars'. It is important to note that most of these are a continuation and refinement of 'average' skills, knowledge and qualities, even though they are cited here for the first time.

'Something special' — advanced facilitation skills

Seen above as an emerging characteristic of 'average' trainers, advanced facilitation skills was singled out as a signature characteristic of the best trainers. These trainers were able not only to smoothly manage an event, they also made participants feel comfortable and could 'hold' a 'safe space' that maximised participants' ability to learn. Furthermore, these trainers were often described as having a special ability to create something even more 'special,' with the skills of 'a showman, performer' who could 'give a performance without being overwhelming,' so that participants still felt welcome and safe enough to ask questions and engage with others, instead of being passive in the face of a 'performance'.

This special ability not only makes for a more effective training, it also helps create an exceptional experience in combination with other abilities, since a training can also be memorable but ineffective as participants forget the content and fail to implement any of the curriculum in their daily lives.

Engaging

Related to advanced facilitation skills, interviewees frequently described 'excellent' trainers as uniquely 'engaging'. The best trainers can connect with an audience and can be so skilled at reading both the group and each individual that they can manage to teach in such a way that each person stays engaged in the process of learning. Tied to this was the ability of the best trainers to facilitate both large and small groups, facilitate rich discussions among participants and foster conditions that helped the most shy and reserved participants feel more comfortable and engaged than they would otherwise have been.

Deep and broad technical skills and knowledge

One interviewee described the best trainers as 'knowing as much about how to train as they do about their subject.' In addition to mastery of the technical aspects of the content, the 'best' trainers are also described as having 'alternate ways of explaining' things, familiarity with a wider selection of tools to offer participants according to their needs, as well as 'alternate methods for doing hands-on work on a particular piece of software.' The 'best' trainers are also

described as not being 'tech heads' and being able to make complicated technology and concepts very accessible to participants. They also tended to model best practices both in and outside of trainings.

Strong andragogical (adult learning) knowledge and skills

These trainers were also described as having a strong understanding of the unique learning needs of adults. They were also described as 'being able to speak human,' and having the agility to tailor for individual participants and peer communities.

Passionate and committed to participants

In addition to their technical knowledge, the best trainers are described as being particularly dedicated to their participants and having 'high standards'. They were described as more regularly conducting research into participants' contexts, demonstrating empathy and often seeing themselves as part of their participants' larger community of HRDs and activists and not 'outside of the movements they work in.' Highly self-motivated, these trainers consistently work hard to get better at what they do. If they did not know the answer to something, they would say so, then follow-up with an answer afterwards. They also tend to be individuals who will identify further opportunities and resources for participants and will work to provide them to participants after the training. They are also described as having a strong web of useful connections through which they can find and provide these opportunities for certain participants in need.

Self-knowledge and self-care

Lastly, the 'best' trainers were described as having high levels of self-knowledge and self-awareness; setting reasonable expectations for themselves and others and practising basic self-care.

The Current Approach to Evaluating 'One-off' Trainings is Broken

Our interviewees described the current approaches to evaluating the effectiveness of 'one-off' digital security trainings—especially *after* trainings have ended—as profoundly broken. There are evaluation approaches that trainers feel work well in limited ways *or* as part of sustained, long-term engagements. But one trainer summed up an almost unanimous sentiment of interviewees: "I don't know any good way to do monitoring and evaluation in a meaningful way."

The reasons for failed evaluation vary, but (as mentioned earlier) one of the most common reasons cited by trainers is that most funded trainings are 'one-off' events that do not include support for trainers to conduct necessary follow-up that simultaneously enables post-training evaluation opportunities. This is in contrast to sustained learning engagements that often include multiple trainings as well as more robust support for HRDs. These not only tend to *have* goals (and an idea of what 'success' should look like), but they also tend to operate at the collective instead of the individual level with wider engagement and support from organisations and networks. All of these characteristics of sustained learning engagements and relationships with participants enable richer opportunities for observation and evaluation in view of certain goals. Aside from communities that already have access to local digital and holistic security expertise, these sustained, long-term learning engagements have been the exception until a number of relatively recent pilot projects, including Hivos' and OTF's Digital Fellowship programmes and Frontline Defenders' Digital Security Consultants.

The difficulties of evaluating the impact and 'uptake' of one-off digital security training events are further magnified by the unique risks of working with at-risk HRDs: responses to requests for information from participants have low response rates, in part due to the need to communicate securely with at-risk participants. This makes effective evaluation and follow-up more challenging for one-off trainings than for sustained, long-term engagements. Because of this, trainers are often limited to evaluating *during* the event, which does not measure or demonstrate post-training outcomes.

Evaluation Approaches Used During Training Events

THE END-OF-THE-TRAINING SURVEY IS A POOR EVALUATION TOOL

In order to ensure a high evaluation response rate, as well as avoid post-training communication challenges, funders, conveners, organisers and training organisations encourage trainers to conduct end-of-workshop surveys as the preferred vehicle for evaluation. However, trainers resoundingly find these to be unreliable sources of evaluation data and 'a waste of time', despite receiving remarkably high evaluation ratings as trainers via this approach.

More than half of the interviewees described the phenomenon of 'gratitude bias' with end-of-training surveys and surveys conducted immediately after the end of a training. One trainer described this well when claiming that the most an end-of-training survey could reflect was:

> *...that people were there. When I finish, people want to pay back with what currency they have, and that currency is kindness, so evaluations are hugely biased towards the positive. And I don't know how to interpret it. Funders love it, but I feel foolish because over 99% are positive — it's like an election turnout in a communist country. (Trainer with more than 11 years of experience)*

Because of this phenomenon, most trainers avoid end-of-training surveys 'unless an organiser asks for them'. If end-of-training surveys are conducted, trainers do not consider them to be useful, valid feedback on their work.

DAILY EVALUATIONS AND TRAINER DEBRIEFS

Described in greater detail in Part 4.2, conducting 'plus / delta' assessments from participants at the end of every day is a valued practice among trainers. Trainers ask participants to share things they thought were good or particularly great that day ('pluses'), as well as anything they would suggest changing ('deltas').

THE LIMITED UTILITY OF PRE- AND POST-TRAINING TESTS

Only three of twenty-three trainers interviewed said they conducted pre- and post-training tests that measured participants' knowledge and skills. While these pre- and post- training tests are valuable and should be tried more widely, it is important to remember that they do not evaluate uptake, nor what is being *implemented* and *used* by participants and their peers after an event, only what they can demonstrate they learned *during* the event. One participant described how much they value pre- and post-event assessments:

> *They've helped a ton, more than I thought, because these are actual questions testing their knowledge. They're mostly general security questions that I ask in different ways before the training, and then [during]. I word the questions differently at the end. Works well and helps you create and adjust an agenda.*

> *Some examples of questions are: What is a firewall? Do you have anti-virus programme? Would having two anti-virus programmes be better than one? What is a phishing link? [Without these], how else would you know how good a training would be? (Trainer with more than 3 years of experience)*

THE RELATIONSHIP BETWEEN 'ONE-OFF' TRAININGS AND FRUITLESS EVALUATION APPROACHES

The majority of trainers say the only usable post-training evaluation data they're able to gather is qualitative, often in the form of irregular follow-up interactions with a minority of past participants. This is considered less-than-ideal, but the best option for gathering data with a higher probability of validity. They also often have pre-event assessments and information about the participants' skills from the training itself for comparison. Despite the shortcomings of this approach overall, one trainer expressed that they would still 'rather get substantive qualitative' evaluation data than glowing, but inaccurate end-of-training surveys.

One of the major issues with this approach is that trainers consider follow-up crucial to the learning and implementation process, but it is rarely supported or funded for 'one-off' trainings. Several trainers reported spending 10-40% of their time conducting unpaid training follow-up for participants, but it is often at the cost of their well-being and livelihoods, as many trainers can rapidly burn out without proper self-care and reasonable work schedules, even at organisations with core funding for training.

Trainings Designed for Individuals Instead of for Organisations, Collectives and Networks

The implicit goal of digital security trainings is to have at-risk HRDs attend workshops in order to understand and improve their digital security. Although these individuals are typically considered to be at-risk because of their activities at a collective level, almost all trainings are designed to target individuals. Nearly all of the trainers interviewed said they either rarely or never had workshops with participants from a single organisation or network (but would like to), and were rarely called in to help an organisation as a whole. Presumably, the *hope* is that this individual-focused model will eventually 'scale-up', either through organisations choosing to adopt and fund organisation-wide improvements, policies and trainings, or through word-of-mouth and social adoption via human relationships and networks. But the prevailing focus on the individual alone does not reflect the reality of how these communities operate:

> *Digital security doesn't exist in a vacuum — it exists in movements. The value we assign to digital security is to support social movements. The movements are the point — securing and strengthening those movements is the point of what we do. So securing movements is one goal, and strengthening them is another... (Trainer with 16 years of digital security training and teaching experience)*

Trainers suspect that not working in a sustained way with committed communities at network and organisational levels means that many of the trainings focused on individuals fail in the absence of a supportive environment where a security culture can grow and thrive.

Barriers to Sustained Leaning and Implementation

Participants don't have peers to implement what they've learned with

Current behavioural research mirrors trainers' own experience-based findings: effective digital security requires collective support, reinforcement, and implementation in order to succeed. Trainers are aware that the heart of this act is at the individual level, with HRDs understanding

their risks and being able to make decisions to effectively reduce those risks, which is why trainings require focus on the individuals' needs and skills. But since security is collective and only as good as the weakest link, the benefits of most current 'one-off' trainings tend to wither at the individual level after a workshop ends without additional follow-up, care, and cultivation. Trainers describe how participants who attend trainings as the sole representatives from their organizations return to environments that don't support what they've learned. As seen in the 'Security in Context' findings, they often don't have peers or colleagues that they can practice using the secure tools and tactics they learned about with. As one trainer put it, "what they've learned will diminish over time since they don't have meaningful ways to implement these things".

No follow-up or sustained support

According to the trainers interviewed for this study, one of the biggest shortcomings of the individual-focused, 'one-off' training model is the lack of post-training follow-up. This critical step, which several trainers described as 'when the real learning begins,Tactical Tech is rarely funded or supported. This only exacerbates other problems with the 'one-off' training model. It also puts an unreasonable burden on busy, committed trainers to provide follow-up *gratis*, which most interviewees reported being unable to do properly or at all.

The heavy burden on individuals to persuade their peers and leadership

Unless a group of HRDs, as an organisation or network, have made a collective commitment to improve their digital security that entails action and implementation of a policy, 'one-off' training participants are having impossible expectations placed on them. They are often expected to implement digital security practices isolated from their peers *and* persuade the organisation to do so as well. Even this approach to capacity-building is usually thwarted by organisations sending participants with the lowest levels of power or decision-making in the organisational structure to digital security trainings. In some cases, trainers report organisations sending participants who no longer work with or for them. Other trainers described organisations that repeatedly send participants to security workshops but make no changes within the organisation.

The current dominant training model used to help HRDs and their peers often places the greatest amount of responsibility for success on individual HRDs instead of distributing it throughout communities. Not all successful digital capacity-building efforts for HRDs require large amounts of 'top-down' funds and support, but they do need to reach a tipping point where the commitment and motivation to improve the collective and individual safety of the HRD community is widely shared throughout all levels of a collective. This ensures that responsibility is distributed instead of centralised on one or two individuals (as 'champions' or in other roles). The findings of this research point to a promising number of ways to explore and pilot new approaches where all members of HRD communities can play a variety of roles in a shared collective effort that is buttressed by sustained long-term learning engagements.

THE INCENTIVES OF ORGANISATIONS AND NETWORKS

It is interesting to note that some of the practices used by established digital security trainers evolved from the circuit riders from the late 1990s and early 2000s; a model wherein an individual technologist would provide ongoing technical support in an organisationally embedded way with a small number of NGOs. Circuit riders conducted sustained work with organisations over long periods of time, which included intensive on-site work, remote support and regular follow-up visits with organisations they developed deep and long-term relationships with.

Today, the spirit and approach of circuit riding has become inverted for digital security trainings and trainers: they almost never work at the collective level, targeting individuals instead, rarely see or experience organisation-wide buy-in and support to improve collective digital safety, and are even treated dismissively or with hostility by organisations. Instead of a deep collaboration with organisations and groups, they are deployed as one-time deliverers of skills and knowledge to individuals at a 'one-off' event. Instead of a shared understanding that adoption and proper use of tools and tactics takes time and support, their body of knowledge is expected to be delivered in as short and discrete a period of time as possible, requiring no post-workshop assistance or support for participants to begin to use these tools correctly or well in their daily lives.

Although seemingly providing an alternative solution to meet the failings of the current status quo, the circuit rider model has been tried and tested numerous times in the context of digital security training and presents a number of challenges. It can lead to organisations treating circuit riders as tech support and not substantially transforming their own skills or practices. It can also expose a group of organisations at the local level by identifying them as having 'something to hide', connected by association. Finally it proves a model difficult to scale on account of the high cost and constricted reach of an individual circuit rider.

Recommendations

Focus on the capacity-building of organizations and networks as collectives in addition to individual HRDs

As discussed at length in the findings, the predominant model of 'one-off' training events that focus solely on individuals is impaired due to the well-established need for groups to collectively adopt practices and tools to enable any degree of privacy and digital security. Furthermore, people are less likely to adopt tools and practices used during social and collective interactions and activities if their peers choose not to do so, are unable to do so, or are even dismissive of or hostile towards them. The current 'strategy' for adoption at the social and collective levels—via individual HRDs who have participated in digital security trainings—isn't the only strategy or the strongest one, especially given the greater range of options and approaches available. Approaches and models for how this can be done need to examine the 'physics' of how the current individual-focused model has failed in order to inform to development of new approaches that can be piloted, iterated, and implemented.

Support the development and piloting of new models for learning and capacity-building

Over the past 3-4 years, members of the global digital security training community have begun to re-evaluate what had become a stale model of 'one-off' trainings, and has found it to be lacking. As described above, this 'old model' of trainings could be briefly described as 'one-off, tool-focused, top-down, and artificially separated' from other security-related realities of HRDs. This relates not only to the design and execution of training events, but also to larger overarching issues of strategy, structural gaps, and programmatic inconsistencies that led to contradictory experiences for HRDs. In aggregate, the findings from trainers in this study as well as from HRD training participants in Tactical Tech's 'Security in Context' study recommend exploring and piloting new models and approaches that provide HRD organizations and networks with sustained learning opportunities over longer periods of time, utilising local resources and expertise more effectively, as well as properly supporting follow-

up when sustained learning opportunities are *not* possible. These would also open up new opportunities for evaluation and assessment unavailable in the current model.

There have been several recent pilots with new approaches for digital security capacity-building within HRD organizations and networks, including several that focus on sustained engagements (examples include the Open Integrity Fellowship Programs led by Hivos and the Open Technology Fund, and Frontline Defenders' Digital Security Consultants). It would be invaluable for the outcomes of these pilots, including the opportunities and challenges encountered, to be shared and discussed with the wider training community.

Additionally, there are structural variations on the 2-5 day 'boot camp-style' training event that warrant greater recognition, experimentation, and evaluation. One approach involves training sessions taking place over a series of weeks, which interviewed trainers reported as being much more effective, as well as less draining for both trainers and participants. It also opens the door to HRDs who are unable to get away from their daily jobs for a week-long training, a model which prioritises individuals who work full-time on human rights issues and can be compensated for their time away. Members of volunteer-based HRD networks find this much harder to do and are often silently excluded from participating in multi-day trainings for this reason. Another variation mentioned by one interviewee is a take on a multi-day training event that leaves the second half of each day open to participants independently directing their own learning or practice with tools, but with trainers available to ask questions or focus on unique challenges or issues. This would help reduce the 'overload' that trainers hear complaints about from participants, who feel that the amount of new information is often too much to absorb in a single multi-day training.

CO-DEVELOP A THEORY OF CHANGE FOR DIGITAL SECURITY CAPACITY-BUILDING

Currently, there is no clear 'theory of change' that articulates how trainings are designed to meet certain goals within a broader process with specific assumptions and preconditions at play. Although the variables, variations, and risks involved in any sensitive work with HRDs naturally lead to uncertainties and safety considerations, interviewees were unable to articulate any discernible over-arching strategic conception of how trainings *worked*. But instead of explaining and defending the vagueness that defines their work, interviewees were frustrated with this situation, and discussed ways that certain initiatives were working to change training for the better.

Working with the wider training community to co-develop of a theory of change would be a powerful community-building and collaborative experience for trainers, both internally and externally. This could begin to articulate a coherent set of achievable goals, including assumptions behind these goals, and how certain actions and activities should be considered preconditions for their achievement. This would also be a rich opportunity to collaborate with (and break down the spaces between) parallel efforts such as software development, advocacy, and other sectors that seek to support HRDs.

Co-develop standards and improve communications and outreach with conveners, funders, and HRD organisations

Trainers consistently reported that digital security training wasn't well understood, deployed, or used by various actors. In addition to the absence of a considered theory of how training leads to a specific set of changes in HRDs' digital security practices, there was also a reported need to standardise training-related definitions and descriptions. There is a clear need for the training community to better define and describe trainings and training-related activities for the rest of the sector. This would also help address what trainers described as challenges with conveners and funders regarding sufficient funding, training design and preparation, participant selection, and more. If conveners and funders have a better sense of what trainings *are* (versus other types of training-related events, such as awareness-raising), how trainings work (best practices and process), as well as what they should reasonably expect outcomes to be, they will be better positioned to convene trainings in a more informed way.

Support collaboration and coordination in the training community

Throughout the interviews, there was enthusiastic support for the emerging environment of collaboration and coordination amongst the wider digital security training community that Tactical Tech has played a key role in, through initiatives like LevelUp. Trainers described how the quality of their trainings had been improved from exposure to adult learning principles, introductions to how psycho-social considerations impact participants, new methodologies and approaches to event preparation and agenda development, and more.

The simple process of becoming part of a community of practice was perhaps the most valued aspect: many trainers feel isolated and lack connections to fellow trainers; others may only know 1-2 trainers to varying degrees and many lacked exposure to their fellow trainers' unique approaches to trainings and professional development. Exposure to fellow trainers and trainings is one of the most valuable means for trainers to learn quickly, otherwise they are only able to learn through trial and error, which comes at a great cost and investment of time. This work has successfully acknowledged trainers and training-related actors as part of a unique, established profession requiring shared standards and professional development.

The trainers interviewed expressed enthusiasm and commitment to existing efforts that seek to bring trainers together and co-develop a shared body of knowledge and professional standards. The existence of such a community also offers up a rich opportunity for co-developing a theory of change as recommended above.