TACTICAL TECHNOLOGY COLLECTIVE

Executive Summary:

Researching digital security training for human rights defenders

Introduction

As technology becomes increasingly fundamental to the work of many human rights defenders (HRDs), a parallel expansion can be observed in the digital threats they face. Tactical Tech has been working in digital security training for human rights defenders for close to a decade, yet whilst the field has experienced rapid expansion in recent years, almost no research or comprehensive review has been carried out regarding the process and effectiveness of current training practices, nor regarding the challenges faced by participants in implementing learnings outside the training room. The two research papers summarised here represent an initial exploration of some if these issues with the intention that the findings will help inform and encourage future applied research projects, the design and testing of new training approaches, models, and curricula, as well as contributing to broader discussion within the digital security training community.

Background

During 2014 and 2015, Tactical Tech undertook two studies into training and learning within the field of digital security for human rights defenders, each broaching the topic from a contrasting perspective: that of the participant and that of the trainer[*].

The first study, '*Digital Security in Context: Learning how human rights defenders adopt digital security practices*' looks at the direct experiences of human rights defenders both in the training room and afterwards. It was initially conceived as an opportunity to examine what key factors influence or improve the uptake of digital security practices by human rights defenders in order to increase the long-term effectiveness of trainings. This emerged from a broad awareness within the training community that time and again tool usage and digital security

* This summary report is based on research conducted by Becky Kazansky and Carol Waters. It was prepared by Hannah Smith. Inquiries about these studies should be directed to Maya Ganesh at maya@tacticaltech.org.

practices by participants either dropped off some months after a training or were not successfully integrated into their working practices to begin with. Although many theories around the reasons for this existed, closer examination of why was required.

The second study, '*Digital Security Trainers' Practices and Observations*' examines the issue from the trainer perspective, centring on trainers' personal experiences, approaches and learnings with a view to sharing and promoting best practices. This developed into a larger discussion of successful approaches, methodologies and personal development stories of digital security trainers. It also examined the influential factors in creating 'successful' trainings as perceived by trainers, as well as practices which could be deemed ineffective or even harmful given the high risks to which human rights defenders are already exposed.

The two studies, though conceived as part of the same process, were conducted in relative isolation of one another and findings were only shared between the researchers following their initial write-ups. Yet taken together, the findings and recommendations of both studies prove complementary and provide a previously unavailable body of knowledge regarding digital security training for human rights defenders.

Below, each study is summarised individually to allow for comparison and contrast of the research methods and findings. A conclusion draws together the key recommendations which emerge from the research as a whole.

Study 1: Digital Security in Context: Learning how human rights defenders adopt digital security practices

This study looked at the question of how human rights defenders adopt digital security practices in the training room and beyond, as well as what barriers they face in doing so.

Research Questions

- How do human rights defenders adapt their digital security and privacy practices to shifting socio-technical contexts?
- How well are individual and collective needs met through current models of digital security capacity building efforts?

Methodology

The research took place over a period of 18 months and draws on findings from interviews, discussions and trainings with a total of 60 people engaged in human rights work. The design was informed by an initial planning workshop hosted in 2013. The workshop gathered 15 trainers and technologists working in the human rights sphere to identify known barriers to effective digital security capacity building. The research itself was then conducted in two phases.

In the first phase thirteen semi-structured pilot interviews were carried out with

geographically diverse human rights defenders, centring around the challenges they face in protecting themselves and their data, as well as the broader context of threats to their safety. During these interviews the participants shared stories of phone-tapping, targeted malware and hacking by state and non-state actors.

The second phase of the research was informed using an action-orientated participatory approach, encompassing the direct training of three human rights defender groups across three countries: an environmental and rights organisation, an ICT for development and human rights network, and a women's and LGBTQI rights network. Written participant surveys were carried out 2 and 4 months after the trainings and follow-up interviews with key individuals provided additional depth and context beyond that which was possible to capture in the surveys.

Key Findings

While each of the groups that participated in the research and training face distinct and context-specific challenges, a number of shared themes emerged. All groups noted a shrinking space for civil society due to constricted funding, new administrative barriers for NGOs and the stigmatisation of rights issues; two groups described a preoccupation by governments with new 'cyber' policies which civil society feels powerless to shape. A common dependency on commercial platforms such as Facebook also emerged, both for connecting with the broader public and for communication within activist circles. This impacted on the way that groups experienced threats and the kind of practices that became a priority in capacity building around privacy and digital security.

With regard to digital security training and uptake of new practices following training, four key challenges emerged which were shared across all groups:

- **Security as a collective practice**

  The study found that security is a robust practice when everyone within the network is communicating securely using the same tools and practices. However, this is often not the case. Frequently only a limited number of people within a network or organisation will receive external training; so, the widespread use of digital security tools remains difficult to promote in the larger network. It is often a security incident or breach which first inspires the need to implement increased security measures; and resistance from key team members can prove a major hurdle.

- **Challenges in using FLOSS privacy and security tools**

  Tactical Tech does not seek to proscribe a fixed set of tools in its trainings. This would neither speak to the swiftly fluctuating technological environment, nor to the key tenet of adult learning theory which highlights the need for training participants to be able to make their own decisions based on contextually driven priorities. Nevertheless, Tactical Tech has established an approach to tool evaluation which promotes the use of free, libre, open-source software (FLOSS) for a number of reasons discussed in the report. The study highlighted a number of barriers to use as experienced by the participants which centred around the following factors:

- Confusion generated by conflicting and/or unsubstantiated information regarding the relative security provided by different software applications (e.g. chat applications)
- Implementation issues related to the need for multiple or all members of a network to be comfortable using a specific software
- Perceived complexity of certain software applications including interface issues
- Lack of clarity on key implementation measures (e.g. regularly updating anti-virus software)

- **Integrating security into workflows**

The issue of integration and sustained usage within networks falls into three categories: sustained individual usage following trainings, spreading learnings to the wider network and the need for ongoing support following the training. With regard to the first, sustained usage at the individual level was facilitated by the following factors:

- Usage not being dependent on others (e.g. KeePass)
- Easy installation process (e.g. Jitsi Meet)
- Heightened sensitivity to changes in social media policies (e.g. keeping track of Facebook's ever-changing privacy policy).

With regard to spreading learnings to the wider network, participants who attended a training often took on the de facto role of security or privacy advocate within their organisations. Some were happy to bear this role, but for others it added extensively to their workloads and put them in a position they were not completely comfortable with.

Participants required ongoing support in terms of troubleshooting, clarification and follow-up on themes which were not covered in the initial training. To test theories regarding added-value, one of the three groups engaged in a follow up training. Participants reported that this helped to solidify skills and aided the process of knowledge transfer within the network. The follow-up training also provided an opportunity to learn new tools that were out of the scope of the first training and gave participants an opportunity to clarify questions about complex or challenging practices and concepts.

- **Linguistic and conceptual differences as barriers to learning**

Within the study, training was forced to be conducted in English, despite not being the mother tongue of the majority of participants. This, while a common occurrence in trainings, emerged as a major barrier to learning not purely because of the linguistic capabilities of the participants, but also because of difficulty in communicating certain technical concepts. Trainers often rely on metaphors to communicate new and complex ideas, but a lack of culturally relevant metaphors can prove problematic. Participants also explained that the translation of tool-related resources and elements within tool interfaces doesn't guarantee the cultural legibility of tools and concepts. Lack of one-to-one translations of key lexicon such as 'protection', 'encryption' and 'surveillance' in local languages is a major barrier to understanding.

Study 2: Digital Security Trainers' Practices and Observations

This study looked at the experiences of digital security trainers working with human rights defenders; what methods and approaches help them to create successful, engaging trainings?

Research Questions

- What factors influence the success of a training?
- How do we know that what human rights defenders learn in digital security trainings helps to them change their behaviour and adopt new and safer digital practices?
- What is the 'after-life' of training?
- What distinguishes an outstanding trainer from an average or poor trainer?

Methodology

The study consisted of semi-structured interviews with trainers that took place over seven months in 2014. Interviewees were selected using snowball sampling, whereby an initial list of possible study participants (based on the professional networks of both Tactical Tech and the primary researcher) was expanded by requesting that interviewees recruit future participants from among their professional acquaintances. Approximately 60 trainers were contacted with an interview request, roughly half responded. 23 individuals were then interviewed. 15 interviews were conducted remotely and eight were conducted in person. Most interviews took place over 90 minutes and the researcher took detailed notes. The notes were then coded for analysis.

On account of the snowball sampling method, many participants had existing ties to and professional experiences with Tactical Tech. In an attempt to reduce selection bias, interviewees with weak or non-existent ties to Tactical Tech were actively included in the sample. The research sample also sought to be broadly representative in terms of geography (country of origin as well as regional focus of trainings), level of experience and gender, although there was a secondary goal to include the most experienced trainers working with human rights defenders globally. Given Tactical Tech's role in the digital security training community as an implementer and intermediary, it enjoys deep and complex ties throughout the training community. Because of this, it was crucial that all interviews be anonymised to encouraged interviewees to speak freely and to avoid exposing or placing at risk the trainers themselves or the communities they work with.

Key Findings

Many differences emerged in the opinions and experiences of the trainers interviewed, including in their preferences for different types of digital security interventions and the perceived benefits of each. However, a number of key findings emerged which can be viewed as supported by the sample as a whole. These included aspects like, in response to the question on what makes for an outstanding trainer, a focus not on individual traits, but on a broader flexibility in approach which enables a more responsive facilitation style and the capacity to cope better when the unexpected inevitably arises. Detailed below are four key findings which can be seen as having wide support within the interviewees.

- **Defining digital security interventions**

  Despite the steady increase of digital and physical security training for human rights defenders over the past 10-15 years, there remain no standardised definitions for the core set of digital security training-related activities and interventions within the broader protection community. Many individuals and organisations regularly use terms for digital security-related activities like 'training,' 'awareness-raising,' and 'training-of-trainers' without a standard understanding of what these mean. For the purposes of the report and to begin establishing a shared understanding, a typology was developed in conversation with the trainers interviewed which is summarised below. Confusion of terms and their meanings was deemed to have negative impacts in terms of meeting expectations and ensuring the value of trainers' work.

  - **Awareness Raising** – denotes interventions of one day or less. Usually such interventions focus on introducing the basic premises of digital security and privacy with reference to some easy-to-implement solutions (such as changing social media settings or installing browser add-ons) but do not tend to include new or more complex security tools.

  - **'Traditional' or 'End-User' Trainings** – denotes interventions of three or more days, typically stand-alone but also as part of an ongoing process. Traditional trainings usually include more in depth transfer of knowledge and skills and often focus at least in part on the hands-on installation and use of specific digital security tools. This necessitates a stricter trainer-to-participant ratio (e.g. 1:8)

  - **Trainings-of-Trainers (TOTs)** – denotes interventions of five to seven days which aim to develop the technical and facilitation skills of potential future trainers. Participants can have varying skill and experience levels, but often have a baseline of technical knowledge and the ability and motivation to expand that in a self-directed way. TOTs require comprehensive preparation and design, including careful participant selection, in-depth pre-training interviews and extensive preparation by the participants. TOTs tend to involve participants designing and leading their own training sessions for fellow participants and TOT facilitators in order to receive constructive feedback.

- **Success factors in trainings**

  Given the multitude of unique environments and continually shifting contexts of human rights defenders, there can be no one-size-fits-all approach. With that in mind, trainers said they found the following attributes led to better training outcomes: good participant selection (motivated by need/risk and with similar skill levels); good preparation; low trainer-to-participant ratio; co-facilitation (training in pairs or teams); in depth understanding of the local context and threats faced; creation of a 'safe space' for training; and planning comprehensive follow-up with participants.

- **Building the capacities of collectives and communities**

  The current dominant training model used to help human rights defenders often places the responsibility for success on individuals. Although these individuals are typically

considered to be at-risk because of their activities at a community level, almost all trainings are designed to target individuals. Nearly all of the trainers interviewed said they rarely or never lead 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. The prevailing focus on individuals does not reflect the reality of how communities operate, nor does it align with the shared understanding that security practices work best when implemented within groups.

- **Broken approaches to evaluations**

  The current approach to evaluating the effectiveness of traditional digital security trainings after a training ends was felt to be profoundly broken. Daily plus/delta assessments - asking participants to share things they thought were good that day ('pluses'), as well as anything they would suggest changing ('deltas') at the end of each training day was a valued and common practice, however the end-of-the training survey was considered to be a poor evaluation tool. In order to ensure a high evaluation response rate, as well as avoid post-training communication challenges, trainers are encouraged to conduct end- of-workshop surveys as the preferred vehicle for evaluation. Yet these are resoundingly perceived to be unreliable; although the tendency is towards remarkably positive evaluations, this was perceived largely as 'gratitude bias' and not as a useful critique from which lessons could be learnt.

Conclusion & Recommendations

By engaging with both trainers and participants, Tactical Tech was able to gain critical insight into the different aspects that foster sustainable and effective training, while identifying persistent barriers to learning and ineffective practices. Naturally, more work needs to be done to assess the extent to which new or emerging training practices counter these barriers and further investigate the security, effectiveness and feasibility of certain tools and technologies.

Based on the two studies, Tactical Tech has drawn together a set of recommendations intended to foster increased sustainability and effectiveness in digital security training.

1. Facilitate closer cooperation in the training community to enable dissemination of best practices and provide a shared advocacy platform from which to engage funders and intermediaries in supporting long-term, sustainable training.
2. Support the development, piloting, and iteration of new training models and approaches which encourage sustained learning with a long-view on impact and effectiveness; build critical reflection into training methodology and develop channels for sharing learnings.
3. Shift the training focus to networks and collectives to foster improved security and sustained tool use through shared practice and workflow integration.
4. Honour the roles which emerge through trainings; improve support for participants who bear the burden of championing digital security within their wider networks.
5. Co-develop a theory of change to position trainings within a more defined, community-wide strategy. Work towards developing a shared lexicon and understanding to improve communication and outreach with funders and intermediary organisations.