Securing Online and Offline
Freedoms for **Women**

Expression, Privacy and Digital Inclusion

Impact Study

Disclaimer

This report has been prepared by Tactical Technology Collective for the "Securing Online and Offline Freedoms for Women: Expression, Privacy and Digital Inclusion" program funded by SIDA. This document also lists the main learning outcomes from the project contributing to the Women's Rights Sector.

The information and views set out in this report do not necessarily reflect the official opinion of SIDA. SIDA does not guarantee the accuracy of the data included in this study. Neither SIDA nor any person acting on its behalf may be held responsible for the use which may be made of the information contained therein.

TACTICAL TECHNOLOGY COLLECTIVE

Sida

Structure of the report

Section 1 is the executive summary of the full report presenting the background, general objectives and main outcomes of the project "Securing Online and Offline Freedoms for Women: Expression, Privacy and Digital Inclusion".

Section 2 summaries the main learning outcomes gained during the project which are divided between conceptual learning and good practices for including gender into training activities.

Section 3 provides an overview of the research activities been conducted as part of the different deliverables composing the project, highlighting in particular the key achievements and outcomes in relation to individual trajectories but also collective actions achieved on the ground.

Acknowledgements

We would like to thank all the GTI participants that have given of their time, personal insights and experiences when answering our requests for documentation, storytelling, interviews and filling out our online surveys. The richness of this report is directly the fruit of this graceful collaboration.

Table of Contents

Glossary

In this study and overall project we have adopted some basic definitions in order to avoid confusion and clarify concepts related to gender, privacy and digital security. The scope of our project consisted in overlapping and interrelating those dimensions together through acknowledging the variety of perspectives and on going debates that shape them as socially constructed visions. In the framework of our study we will define some of those concepts as follows:

Anonymisation is the process that ensures users to remain anonymous as they access and use the internet by either encrypting and removing personally identifiable information.

Encryption is a way of using clever mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key.

Social networking platforms or social media, are online tools that offer several functions to network among users by creating, sharing and exchanging contents (text, images, videos, etc.). They can be commercial (in which case they tend to profile their users), or autonomous and community-driven.

Online identity is a set of data and features defining how every internet user presents themselves in online communities and web services. Sometimes it can be considered as an actively constructed

presentation of oneself and compared to a digital version of a social mask.

Liberating technologies can be defined as appropriated technologies that do not harm, are rooted in the free software and culture principles and are designed by default against surveillance, opacity, programmed obsolescence.

Holistic security are interventions and practices which ensure the agency, safety and well-being of activists and human rights defenders from a more holistic perspective; one which includes the physical, psycho-social and digital aspects of security.

Safe spaces share common values and enable members of a group to flourish, empower themselves and create community.

Gender roles are sets of societal norms dictating what types of behaviors are generally considered acceptable, appropriate or desirable for a person based on their actual or perceived biological sex. These are usually centered around opposing conceptions of femininity and masculinity, although there are myriad of exceptions and variations.

Intersectionality or intersectional feminism argue that feminism cannot be studied, understood, or practiced from a single, immediate, standpoint; understanding requires engagement with culture, class, sexuality, ethnicity, gender and other power structures which engender inequality.

Cis-man is a man who is naturally-born as a man and self-identify as a man. "Cis" is the opposite of "trans". We can also see cis-women, cis-Gender, cis-men, etc.

LGBTQIA is a common abbreviation for lesbian, gay, bisexual, transgender, queer, intersex and asexual community.

Transgender is a person who lives as a member of a gender other than that expected based on anatomical sex. Sexual orientation varies and is not dependent on gender identity.

Trans* is a prefix used by those who do not self-identify as a cis gendered person, which means that the gender (or lack of it) that they identify with, doesn't align with the gender they were assigned at birth. The asterisk indicates that trans* is an umbrella term for all the diverse possibilities of gender identities and non-identities (for example, some might be boi, trans woman, gender-fluid, transvestite, genderqueer, two-spirit).

Acronyms

The table below presents the main acronyms used in this report.

Acronym	Detail
ADIDS	Activity – Discussion – Input – Deepening - Synthesis
DS	Digital Security
DST	Digital Security Training/Trainers
FOSS	Free and Open Source Software
GTI	Gender and technology Institute
ICT	Information and Communication Technologies

LGTBIA	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex and Asexual
PA	Privacy Advocacy
STEM	Science, Technology, Engineering and Math
WHRD	Women Human Rights Defenders

Section 1 - Executive Summary

Tactical Tech implemented the project entitled 'Securing Online and Offline Freedoms for Women: Expression, Privacy and Digital Inclusion' during the past year from June 2014 to July 2015. Our work in 2012 and 2013 carried out under the SIDA-funded Tactical Tech project; 'Strengthening and Securing Net Activism: Enabling actors for change to increase the free flow of information and Freedom of Expression online' laid the foundations for this project. In both phases we have been able to adapt our work, allowing us to engage directly with women human rights defenders (WHRD) and women net activists in order to face a global trend of using ICT for controlling and shutting down women voices and opinions through online harassment and gender-based violence launched by governments and non state actors.
We have worked to build capacity within the sector and provide practical solutions and advice to women who use the internet intensively to carry out their activities. The project was designed in the long term to increase our target groups' resilience and their capacity to develop their own mitigation strategies by shifting expertise to the community itself. In a multi-faceted approach the project has directly strengthened people's capacities to firstly improve their own response to restrictions to freedom of expression and freedom of opinion and secondly enable them to improve the capacity within their own communities. Our research and experience shows that only project activities that are embedded in and owned by the communities take hold and stand a chance of succeeding in the long run.

This project is therefore a practical response to demand on the ground and is based upon Tactical Tech's theory of change and its 'do not harm'

approach which puts the safety and wellbeing of target groups and the specific communities they represent at the centre of all activities.

In a nutshell, this project has enabled us to train 48 women in becoming privacy advocates (PA) and/or digital security trainers (DST). As a prolongation of their training, participants to the Gender and Technology Institute (GTI) have organised at least 50 activities across 18 countries dealing with gender and technology, privacy and digital security within their own organizations and/or communities. Those awareness and training skills activities have directly reached 1,324 persons. All together they have raise awareness and contribute to skills building on the ground enabling more women to protect their privacy and engage with security tools and practices.

Our learning online and printed resources have been accessed by at least 14,000 persons from the global South during the twelve months of development of this project. The learning resources included our Women Rights Info Activism Toolkit"[1], the guides for LGBTI in MENA[2] & sub-Saharan Africa and our manual for including gender into privacy and digital security entitled "Zen and the art of making tech work for you".[3] The project also included the development of a wiki platform[4] which provides women net activists and human right defenders with comprehensive resources on digital security and privacy activities with a gender focus. This online resource, produced in collaboration with women from 22 different countries documents over 60[5] workshop

1 https://womensrights.informationactivism.org/
2 https://securityinabox.org/en/lgbti-mena
3 https://ttc.io/zenmanual
4 https://gendersec.tacticaltech.org/
5 https://gendersec.tacticaltech.org/wiki/index.php/Category:Activities

and trainings organised on the ground. It also includes 36 tutorials[6] on how to teach others about topics related to gender and tech, privacy, holistic and digital security; 21 how-tos[7] for self-learning about those topics.

All these outcomes have far exceeded the objectives and targets established in our results framework proving that investing in WHRD and women activists' skills generates important social returns. This impact study includes the analysis of a sample of participants and activities which is larger than originally anticipated and it presents an exiting panorama of ground-based work for including gender into privacy and security.

Milestones

In September 2014 the open call for applications to the Gender and Technology Institute[8] (GTI) was launched and distributed among our networks. In less than six weeks over 350 applications were received. Applicants lived in many areas of the world and represented different socio-demographic and political backgrounds. However their personal stories in relation to privacy and digital security threats faced by themselves, or their communities, were disturbingly alike.

Online threats and gender based violence trap too many women into a contradictory situation in which on one hand the use of the internet is crucial for their work and/or activism, in order to coordinate actions,

6 https://gendersec.tacticaltech.org/wiki/index.php/Category:Tutorials
7 https://gendersec.tacticaltech.org/wiki/index.php/Category:How_To
8 https://www.tacticaltech.org/gender-tech-institute

enable a wider reach out, display new identities, and on the other hand they are also increasingly exposed to surveillance, harassment and punitive actions. All these factors have led to a situation in which the internet is not a safe space and in which it is common to see women's work and voices being deleted, (self)-censored, and actively prevented from being seen, heard or read.

Answers to our call for applications echoed this situation and while many applicants reflected on the stereotypes and prejudices they had face when engaging with tech, there was also a general acknowledgement of a lack of security (either digital, physical or well-being) of women when accessing, using and developing technologies. Besides, the use of tech to undermine privacy and create new forms of surveillance and control over women bodies and opinions was also remarked. Among women targeted, the WHRD and LGTBQI activists working on gender social justice issues or sensitive topics, such as health, reproductive and sexual rights were felt as particularly at risk. Moreover, vocal women, such as bloggers and journalists engaged in politics or feminist issues were also cruelly under attack. As put up by one of the applicants:

> "Women's rights Activists lose the opportunity of having a personal and private life because they are closely monitored"

Testimonials showed that technology-related violence is located on the continuum of gender-based violence, making clear the structural aspect of violence by linking, expanding and/or mirroring online attitudes with

offline prejudices. Stories depicted attacks in the form of smear campaigns, identities theft, doxxing and leaking of intimate and/or personal details, "revenge" porn, blackmailing, hijacking of devices and social media accounts and calls for violence such as rape or death.

> "I live in a country in which a man may **kill his wife because she has a Facebook** account"

> "The general theme of surveillance was a background in my life, **I come from a conservative family** and what I said, what I wrote, talked on the phone and things like that were under surveillance"

These **attacks have been related to governments, hate groups and also relatives that are using technologies** to intimidate, harass, track them down because of their gender and/or sexual orientation, their opinions and activism. It is noteworthy that many applicants also pointed out the responsibility of ICT-companies and social media platforms related to monitoring, selling of data and information provision to governments. Their **failure in creating policies or regulatory mechanisms for tackling abuse**, and pervasive and rampant online misogyny, bigotry and gender-based violence were also frequently underlined.

Many applicants also felt that they were under attack from different

social groups. The 'known' ones such as families and partners and the 'unknown' ones such as governments, hate groups or and criminal organisations. In the latter case, it was more difficult to clearly assess who they were and how much tracking and monitoring they were undertaking. The lack of understanding about the "things that were really happening" and the uncertainty about who were responsible were also frequently reported.

> "How can we communicate safely **without fearing for our lives**?"

> "The situation is becoming more alarming than before and the climate of **fear is increasing day by day**. Women are bullied worse than anyone else just because they are women and should follow the norms on how to be a good woman".

These testimonials also showed that applicants **relied on a tactical use of internet** for building reputation, networks and achieve social transformation. At the same time they were **increasingly aware that maintaining their privacy and digital security** was crucial for keeping up with their activities and activism online and offline. Consequently, those needs led to a clear demand for more adapted methods and tools but also for safe spaces and availability of time to sort out their doubts and learn to overcome the most unpleasant aspects of their relations

with ICT. The lack of privacy and security that many applicants were subjected to, also meant a lack of spaces in their own local contexts where they could gather and learn about new privacy and security tools and practices. Solitude and isolation were expressed and many statements referred to their feelings of "being the only one paying attention to those issues" and the fact of not having nearby trusted people and networks that could support them in learning more on those topics.

The Gender and Technology Institute

Figure 1: Picture of GTI participants

The aims of the institute were to train participants in order to learn tools and techniques for increasing their understanding and practice in digital security and privacy and in order to become digital security trainers and privacy advocates within their own organisations and communities. The Institute was also intended to better understand what could be new approaches to privacy and digital security including a gender and cultural diversity approach. Contents addressed encompassed theoretical elements dealing with gender and technology, privacy and surveillance, training skills and practical tips and methodologies to become an outstanding privacy advocate or digital security trainer. Other dimensions, such as holistic security, self care, risk analysis, tackling online violence, develop feminist principles

of the internet were also discussed along the encounter.

In order to plan the engagement with communities, training methodologies, curricula, contents and the security measures that should be adopted for the organisation of the GTI, an international kick off meeting was organised in October 2014. It was attended by 21 WHRD, women net activists and digital security trainers, who presented their experiences in relation to gender, security and privacy, and brainstormed about methodologies and session planning to prepare the agenda. The interaction with the selected participants, criteria for selection and how to ensure their safety before, during and after the GTI were also addressed. Finally, creating a safe space and an atmosphere of wellbeing and relaxation during the event was also discussed in-depth.

Our evaluations of applications used a data audit appraisal to check their suitability to the aims of the institute and the ideal-types of participants defined in our call. The data audit was achieved in two rounds, one first step was applied checking for their legibility and enabling us to extract a more reduced pool of motivated and adequate potential candidates. In the second step another set of criteria was applied in order to ensure as much diversity as possible among participants.

Some of the criteria used were: Living and/or working in the global South, acting as a social change agent, being connected to different type of communities, networks and organisations, english fluency, motivation to apply, experience with training, digital security and privacy tools. The originality and uniqueness of the applicant experience, inasmuch as the soundness and consistency of the application were also evaluated. The second set of criteria consisted in

achieving as much cultural diversity as possible among geographical areas (MENA, sub Saharan, post-Soviet states, South & South-East Asia, Latin America and the Caribbean region), among various gender based identities, among activists and representatives of an organisation and among types of organisations (aims and target audiences). Organisations, informal networks and individuals with a demonstrated grassroots reach were prioritised.

Whenever possible, and dependent on availability of secure communication channels, the GTI preparation included for all invited participants a skills and learning needs assessment. Some of the information gathered dealt with: Basic computer and/or mobile phone habits, technical knowledge, contextual, cultural and social information, perceived threats to digital security, and information about any attacks participants could have been subjected in the past.

We complemented these with peer to peer conversations between facilitators and future participants. This type of personalized

attention proved to be especially important in creating trustful relationships with new participants who had never worked with Tactical Tech, or had never joined a training, traveled abroad or felt more shy about spending time with strangers. Even though highly time consuming, it provided important outcomes by helping to remove possible barriers and fears, setting expectations, experimenting directly with new means of communication and overall, by involving as soon as possible the trainee in co-owning her training process.

> The methodological framework adopted during the GTI was based on the basic principles of adult learning. Most specifically the ADIDS method that stands for Activity-Discussion-Input-Deepening-Synthesis which is frequently used in awareness-raising workshops on specific social issues. For digital safety training, which mixes both awareness-raising on issues and teaching technical and strategic solutions, the ADIDS methodology is a good fit.

Finally, this approach was complemented with a feminist approach engaging with long time methods, such as shaping safe spaces, understanding ones privileges, putting attention on power and inequitable relationships, creating nurturing and inclusive processes for reflexion, exchanges and learning. More specifically feminists critics and perspectives of technology and how women are already self-including themselves in those fields were transversally addressed during the GTI. Because of that almost all facilitators were women already engaged for a long time in using, developing and training others to technologies.

Section 2- Learning outcomes

In this section we present the main **learning outcomes** gained during the project and the good practices that were identified in relation to providing training to privacy and digital security from a gender perspective. As explained in the previous sections, this project enabled the creation of **a global exchange among WHRD and women net activists coming from 30 different countries** about how we could develop practices that enable those and other groups at risk to include privacy and digital security into their lives, and how could we create social processes to keep on learning while helping others to learn about those concepts, methods and tools once back home.

The following ideas are based on the exchanges maintained during and after the Gender and Technology Institute, and on the great amount of past and current on-going research, experiences, initiatives and policies that are being developed to overcome specific challenges posed by the interactions between gender and technology. More specifically, we have developed an international review of women and feminist initiatives[9] that are tackling gender discrimination and violence through an intensive and creative use of ICT and Internet. Besides that, the peer-to-peer and group learning processes derivative of the experience gained by participants through the organization of more than **50 local activities targeting women, activists and LGTBIAQ** also document this learning paper.

Recurrently, the following challenges were pointed out by GTI participants as **major bottlenecks for becoming privacy advocate and/or digital security trainers:**

- **Late and/or controlled access** to Information and Communication Technologies (ICT)
- Reduced or **difficult access to privacy and security tools** and technical knowledge associated to it
- **Lack of safe spaces** (online and offline) and trusted networks for

9 https://gendersec.tacticaltech.org/wiki/index.php/Gender_and_Feminist_Initiatives

learning more about privacy and DS tools and practices

- **Fragmented and precarious lives due to activism** or work in human rights issues
- **Exposure to surveillance** and online violence often related to activism or work in human rights issues
- **Deficient individual and collective self-care** and wellbeing practices

In the following, the focus will be on detailing the main learning outcomes that came from analising those challenges. **We first detail the relationship between gender roles and violence against women and technology, second, we point at the need to reframe the debate from exclusion and discrimination to inclusion and self-inclusion.**

In a nutshell, we can say that **including gender into privacy and security requires intersectionnality** which means to engage with the diversity of cultures, social status, gender identification, sexual orientations, race, ethnicities and other power structures that create various forms and levels of inequality for individuals and communities into their access to security tools and practices. Intersectionality refers to a corpus of theories and practices that state that oppression within society, such as sexism, racism, biphobia, homophobia, transphobia, and belief-based bigotry, do not act independently of one another. These forms of oppression interrelate, creating a system that reflects the "intersection" of multiple forms of discrimination.[10] Intersectionality goes hand by hand with a gender lens because both require us to understand our privileges in any of the different dimensions of our social lives.

10 https://en.wikipedia.org/wiki/Intersectionality

The women who attended the GTI network have indeed many identities that can relate to their ethnic background, age, geographical location, economical situation, political and inner beliefs, sexual orientation, professional status, mobility capacities and a long list of other elements. Accordingly when assessing the risks they are exposed to and the strengths they have, which constitute the basis of any travel journey towards privacy and digital security, they are required to take into account all them.

Additionally, the integrated (holistic) security perspective seeks to overcome the unhelpful separation between approaches which focus on digital security, personal/organizational security, and psycho-social well-being.

This involves recognizing the effect of stress, fatigue and trauma on activists abilities to engage with 'rational' processes of risk analysis, security planning and skill building in digital security; furthermore, it recognises the impact of new technologies on our ability to accurately perceive indicators of danger and take action to stay safe. Many participants felt that an integrated approach to security made more sense with many of the groups that were trained on the ground such as indigenous groups, women in rural and poor areas, LGTBQ, sex and health activists, anti mining and environmental activists, journalists and community champions. An integrated approach enables participants to think about how threats relate to each others and which security practices help them to transform their loneliness and individual fears into collective strategies to overcome dangers and creating protection among the members of a connected network.

Figure 2: Picture of Enredadas, an initiative of one GTI participant

All together, through this project we also discovered that enabling enthusiasm for privacy and digital security practices required an integrated approach linking those to our well-being and physical security as human right defenders and feminist and queer activists. By exposing the many invisible contributions that sustain digital security communities, avoiding frustrated expectations, gaining self confidence and losing fear through do-it-with-others processes, gender and cultural diversity in those fields can be included. Accordingly, adapted, updated and targeted resources and training methodologies focusing on specific threats and strengths is required in order to activate curiosity and better understanding through contextual references.

Gender roles and Violence Against Women along the technological cycle

Gender roles are sets of societal norms dictating what types of behaviors are generally considered acceptable, appropriate or desirable for a person based on their actual or perceived biological sex. These are usually centered around opposing conceptions of femininity and masculinity, although there are myriad exceptions and variations. Therefore the first step for including gender consists

in acknowledging the gender roles that society attributes to us at birth and during the rest of our lives and that generate stereotypes that can become prejudices and misogyny. Looking at these threats and exclusion from an intersectional point of view, we can furthermore see that they are often aggravated by other forms of social exclusion such as socio-economic status, place of residence and/or socio-demographic factors such as age, ethnic origin or sexual orientation. All together they result into specific threats and violences against women, queer or non-binary persons along the complete technological cycle, which encompass the following dimensions:

The production of technologies

As Wilding and Fernandez already stated in 2002, "*we need much more research on the specific impact of ICT on different populations of women whose lives are being profoundly altered by the new technologies, often in ways that lead to extreme physical and mental health problems*".[11]

Electronics and telecommunication industries are highly dependent on low-wage workers and often operate in special economic zones known for their anti-union measures. In Malaysia, between 70 and 80% of the workforce in this branch are women, who are also often immigrants. In Mexico, women are reported to be 70% of the workforce and are forced to work overtime and often face sexual harassment from their direct superiors among other systemic violences. Currently, there is a lack of networks and initiatives that can challenge those conditions and reclaim technologies produced and recycled in fair working and environmental conditions.

Including gender requires taking into account the general context of human rights violation taking place in most of the areas where ICT is assembled, and also where its components are extracted. Current large production of the technologies we consume and use in a daily base is based on a set of structural violences against women.

11 Situating cyberfeminisms, Maria Fernandez and Faith Wilding, Domain errors book: http://refugia.net/domainerrors/DE1a_situating.pdf

Access to technologies

The gender gap in relation to access to technologies can be spotted when asking women about their first memory of a technology and how much life distance they traveled until they became active users of ICT. This amount of years between our first memory and when we started to actively use ICT represents our gender time gap in relation to access to technologies.

Moreover, the digital divide is still largely happening between urban and rural areas and it is also strongly gendered as current data estimates that there are 200 million fewer women connected to the internet than men.[12] This lack of access can be caused by a deficient connectivity or inexistent infrastructure or by a lack of inclusiveness and usability in the design of technologies, and it can be also aggravated by discrimination pushing away or forbidding women to access ICT, denying their basic rights to communication, information and knowledge.

Therefore including gender also requires us to understand how different women in different conditions find ways of accessing technologies, even if they are not supposed to or supported in doing so, and how they can protect themselves and others in the process.

Uptake of technologies

When finally uptaking with ICT, we may face violence online because of our gender and/or sexual orientation. As explained by Jeniffer Radloff from the APC women programme: "*What is now increasingly obvious is that the Internet and digital tools and spaces have a profound impact on the magnitude of threats and have simultaneously broadened and increased the kinds of surveillance and harassment to which human rights defenders, both men and women, are being subjected. Attacks against women are invariably sexualised and WHRDs*

12 Doubling Digital Opportunities: Enhancing the Inclusion of Women and Girls in the Information Society, (2013) ITU & UNESCO

are often more at risk online (as they are offline) than their male counterparts. Invariably they can experience more hostility, and at the same time lower levels of protection, compared to their male colleagues".[13]

The problem of **online harassment and threats against women and their collaborators**, coming from both governments and non-state individuals and groups, has **become more visible in the last few years.** The internet is not a safe space, and it is all too common to see the work of women and activists being blocked, deleted, (self)censored, and in general, actively prevented from being seen, heard or read. Consequently, these trends **diminish both the freedom of expression and privacy rights of the people targeted.**

Including gender requires us also to tackle specific gender-based online violence and to build capacity on the ground so that women and minorities can protect and strengthen their freedom of opinion and expression.

Development of technologies

In a 1991 essay, Ellen Spertus[14] examined the influences that discourage women from pursuing a career in a technical field, more specifically in computer sciences. These influential factors range from the different ways in which boys and girls are educated, the stereotypes and subtle biases female engineers face working in predominantly male environments, sexism in language and subconscious behavior that tends to perpetuate the status quo. The lower levels of women in Computer sciences and STEM studies and in

13 "Digital security as feminist practice", Jennifer Radloff: http://agi.ac.za/sites/agi.ac.za/files/standpoints_digital_security_as_feminist_practice.pdf

14 "Why are There so Few Female Computer Scientists?", Ellen Spertus: http://www.spertus.com/ellen/Gender/pap/pap.html

related professions within the ICT industry have been intensively studied. There is considerably less literature on the participation of women in **"free software" communities and hacking cultures**, or on the introduction of women into software and technologies development thanks to informal learning processes in voluntary and/or activists contexts.

Besides that, the documentation of women contribution through history to the design and development of technologies is still very scarce, anecdotal and often derivative of a negation and invisibility of women roles in those specific histories. This drives in turn to a lack of role models and the impossibility of launching new imaginaries and overcome current stereotypes.

Including gender also consists of researching the **HerStory and making women, trans* and queer experiences** in the management and development of technologies visible, be those digital ones, or **appropriated technologies such as permaculture or health and self-care technologies** for instance.

Governance of Internet and ICT

We also must claim the power of the internet to amplify alternative and diverse narratives of women's lived realities'. As underlined by Valentina Pelizzer Hvale, the feminist principles of the internet "*cannot turn into an ideology but need to be an open evolving platform. A space of agitation and construction of political practices so that the internet facilitates new forms of citizenship that enable individuals to claim, construct, and express their selves, genders, sexualities. And it is precisely for this reason that we should not confine ourselves to the use of internet as a tool but must understand, monitor and engage with those who govern the internet*".[15] Now its governance is a very complex universe, a decentralized and international multistakeholder network of interconnected autonomous groups drawing from civil society, the private

15 "A feminist internet and its reflection on privacy, security, policy and violence against Women", Valentina pelizzer hvale: https://gendersec.tacticaltech.org/wiki/index.php/A_feminist_internet_and_its_reflection_on_privacy,_security,_policy_and_violence_against_Women

sector, governments, the academic and research communities and national and international organizations. Besides, it is also important to influence policies within the social media platforms we are actively using to present ourselves online, coordinate and network with our different social networks composed by our families, colleagues, activists friends.

Because of this, **including gender is also about enabling a greater participation of women, trans* and queer into institutions contributing to the governance of Internet inasmuch as inside companies delivering services for supporting our networking and online identity.**

The end of life of technologies

Finally, we should not forget about the e-waste dump routes that consist on those areas where electronic waste is shipped, often contradicting the principles settled by the Basel Convention[16], and that conclude in their abandonment in developing countries where local communities have to take in charge of their recycling, generally under very poor ecological, social and working conditions. Those places represent the **end of life of technologies** and another problematic aspect of consumerist and fetishistic approaches to ICT.

From exclusion and discrimination to inclusion

This review of the steps composing the technological cycle shows that including gender into privacy and digital security requires us to first acknowledge that gender gaps, discrimination and violence against women are happening along the process in a structural way and that they influence the conditions of women, trans* persons and at risk minorities in relation to their experience of/with ICT. It also shows that when we use technologies, we should reflect about how those are liberating or alienating for other groups and

16 http://www.basel.int/

individuals.

> Liberating technologies can be defined as those that are designed mindfully, fairly produced and distributed, are rooted in free and open-source software principles, are not designed for 'planned obsolescence', and are built to be secure by design. In the same spirit—but ultimately determined by what users do—that the technologies, systems, and digital services we choose are not designed for or are resistant for use in gender-based violence and surveillance.

In any case, to stop exclusion is not the same thing as achieving inclusion. Focusing on exclusion might lead us to believe that inclusion is impossible, when there are actually women who include themselves in ICT and digital inclusion actions and policies that have been effective. There is a need to shift the question from why women or trans* persons do not access, use, study or work in ICT to the question of why, where and how we have become involved in ICT and have been welcomed to it. This becomes more consistent with feminisms that consider the experiences of women and trans* persons at the heart and point of departure of our reflections and have brought to light the contributions, uses and desires we make of ICT. With this, role models for many more could be put in the spotlight, as well stereotypes about gender and ICT could be weakened.

Enabling the inclusion and self-inclusion of women, trans* and cultural minorities in ICT is firstly a question of gender justice and equality. However, there are many other arguments that support an improved inclusion in ICT. Increasing our representation in ICT also increases the pool of skilled IT workers, and privacy and digital security developers and trainers. Moreover, this means to work in sectors with higher pay and prestige and at the cutting edge of current changes. Including women and trans* persons in ICT would

also make possible more diversity of profiles developing ICT and the information society in general. This would include the voices, perspectives and needs of thousands of potential users, as well as it would possibly create more opportunities for technological products that are extensive, adaptable and appropriated to many different profiles while, at the same time, facilitating the development and transformation of the ICT sector itself and society as a whole.

Self-inclusion mechanisms

When referring to self-inclusion of women and trans* persons in ICT we position ourselves as agents conducting our own ICT inclusion and focus on the mechanisms that we activate and/or decide to follow, to contribute to and transform ICT. The main self-inclusion mechanism commonly stated consists of learning. However, many women do not learn in formal education nor study engineering, but engage in non-formal, informal learning processes and often volunteer activities. In addition, as in many other sectors, women and trans* persons seek and access ICT jobs and activism to self-include themselves in ICT. However, due to gender stereotypes we can find it difficult to engage in self-promotion or in making visible our contributions.

When finding barriers in a given context or seeking new opportunities most of the women and trans* persons have opted for mobility, both occupational and geographic, low profiling or opting out. Many of us have also become entrepreneurs or tech related activists to carry out our ideas and projects, alone or with other partners, to maintain and continue our ICT practices, as well as setting plans, actions, organizations and build new networks. In relation to that, we have been collaborating and sharing knowledge but also works, codes and resources that could help and be used by others. Through collective participation we learn, interact and generate new projects as well as new forms of inclusion.

Previous experiences related to gender inclusion have identified a number of auspicious factors facilitating the entrance and immersion of women and

minority groups in technology. In a nutshell main recommendations for the inclusion of more women into tech related fields are:

* Facilitate women and trans* persons' access to ICT.

For example: encourage your daughter or student, create pedagogical materials on gender and ICT, share your mouse and tools with her, and collaborate with collectives that work on equality.

* Make visible, create awareness and recognise women and trans* persons' contributions.

For example: Pay attention and visualize their past and present experiences and achievements. Give credit and promote their contributions and their diversity.

* Create gender friendly environments.

For example: implement a welcome policy, encourage work-life balance measures, say no to sexist jokes and fight against any type of harassment and violence.

* Mentor and sponsor.

For example: Offer yourself as a mentor and share your knowledge without patronising her. If an interesting new role is vacant, point to her as a candidate.

* Practice Feminism, Let us be and transform.

For example: Do not expect what has been traditionally there. Be open to non linear trajectories, to new uses of old tools, other and new ways of doing and living gender identities.

In conclusion, while it may not be possible to stop online harassment and gender-based online violence yet, we can certainly raise awareness, provide practical solutions and create new strategies for securing online and offline freedoms for women and trans* persons. This involves broadening the focus of policy discussions from girls' and women's access and use of technology to include technology-related violence as part of the continuum of gender based

violence. Those creative solutions also depends of careful planning for creating partnerships, synergies and networking among organisations that have been for working on gender based online violence, how to research, document and overcome it. Accordingly, this project is also informed by the advocacy of groups like APC and others, who are working to reframe internet rights as human rights.

Figure 3: Imagine a Feminist Internet by APC Women Program

Good Practices for trainings with a gender perspective[17]

Our experience in the field indicates there is no single one size fits all model for privacy and digital security training activities including a gender perspective and that sustainability is a multidimensional construct that requires a good understating of the organisational, human and technological aspects of those initiatives. To improve their sustainability it is crucial to establish social mechanisms and learning communities around privacy and digital security which contribute to breaking the circle of isolation and maintain the motivation amongst social change agents to engage with these fields. In regards to these needs, peer to peer exchanges processes (mentoring, tutoring, supporting) are key in enabling participants to remain tuned and motivated to engage. We list below the other elements that we have identified as good practices for including gender into privacy and digital security trainings and for increasing the sustainability of those initiatives on the ground:

Dedicate resources to long-term planning of learning interventions: Our engagement with groups reinforced the need to reserve adequate resources to plan trainings and other learning interventions to include activities before, during and after the training. We believe this planning should be done together with local points of contact to ensure that the intervention meets the priorities of groups.

Prioritize relationships: Strengthen existing relationships and foster new social connections. Participants consistently expressed a view that a key barrier to adoption of digital security tools is the fact that there is often no one to use these tools with. They are also not introduced to any tools that might facilitate group communications. This is not only a practical barrier but also affects people's attitudes of their own agency over their digital security and

17 Those good practices are based on a Tactical Tech research study entitled "Security in Context" (publication forthcoming 2016) and have been adapted to the "Securing Online and Offline Freedoms for Women: Expression, Privacy and Digital Inclusion " impact study.

privacy. It also means that an unrealistic level of responsibility is placed on individual human rights defenders.

Focus on the collective instead of the individual: The currently funded model and approach that focuses on the individual is crippled from the start given 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 hostile towards doing so.

Support sustained learning: For any sort of sustained uptake, one training serves as the basis for learning but a second training provides the space and time to solidify skills, strategise at a movement, network or organisational level, and to support the growth of champions.

Honor fluid roles: trainee, trainer, champion, advocate: As with any complicated, challenging, and constantly evolving effort within both larger and localized efforts of networks working towards their goals, the range of roles for individuals goes far beyond the two roles of a "trainer" and a "participant." Although these well-worn designations arose from the need for skills associated with "trainers" by "participants" in need, the sector is overdue for a re-thinking and consideration of how best to distinguish the crucial roles played by individuals who do not easily fall into either category. We observe that funders and members of the trainer community often conceive of the training of trainers event as the most appropriate place to focus on strategies for communicating concepts and tool-based skills.

Contextualise digital security concepts: Many of the frames and metaphors we use to describe technologies circulate through commercial business models. Technologies have a contextual origin, but cultural influences can get lost within discussions about the global nature of networked technologies. The global framing of networked technologies can obscure the ways in which the development and adoption of technologies is informed by specific geographical, linguistic and cultural factors. Interviewees emphasized the importance of drawing on local meanings to discuss concepts around privacy

and digital security.

Address digital literacy: In cases where digital literacy is low among groups working together, they may want to prioritize training on these skills amongst a broader audience, along with deepening more specific skills which rely on difficult tools such as PGP. Building digital literacy makes it easier to spread practices.

Build strong infrastructure for learning and support: It is vital to establish a set of best practices for handling information and protecting communities for funders, trainers, and intermediaries engaged in digital security capacity building. Capacity building around privacy and digital security has groups, trainers, and funders in constant communication with one another, during which sensitive information may be exposed.

Involve participants in the development of learning resources: It is important that participants co-own the process of developing, testing and distributing learning resources that meet their local and communities needs. Those resources should use a gender sensitive language and include examples showing the richness and diversity of women and trans* contribution and involvement with technologies.

Explore inclusive strategies for evaluation: Because situations change so quickly, and appropriate security practices must be based on changing context, it can be very challenging to establish a baseline upon which to evaluate the effectiveness of trainings. The effects of trainings play out over longer periods of time, which is part of what makes evaluating their effectiveness challenging. Learnings gained from skill transfer in trainings may become relevant long after, as in the case of one HRD who used a technique to document incidents in order to create a collaborative strategy for a network of organisations.

Section 3 - Life trajectories - Distances traveled
Research design and methodological framework

Tactical Tech's theory of change is based on the development of projects designed for directly strengthening people's capacities to firstly improve their own response to restrictions to freedom of expression and freedom of opinion and secondly enabling them to improve the capacity within their own communities. Our research and experience shows that only project activities that are embedded in and owned by the communities take hold and stand a chance of succeeding in the long run. Accordingly, the key research questions underlying this impact study are:

- What has been the social change achieved by the project? And what have been the distances traveled by its participants?
- How investing in WHRD skills and capacities improves their opportunities for self-inclusion into the privacy and digital security fields?
- Finally, how can we ensure that positive mechanisms keep responding to people's needs at critical moments during their inclusion in those fields? And what can we learn from this first year for the development of the program the next three years?

These research questions have been constrained by our working and training methodologies based on the 'Do No Harm' approach which implies that we create a specific framework for engagement that details criteria for decisions made about the well-being of participants and partners.

We place a priority on the co-understanding and sharing of methods and aims between Tactical Tech and its trainers and participants at events. We adopt an explicit consent model by informing participants about the intentions and expected outcomes of interventions; this consent also implies the choice to not engage with activities. Do No Harm also means that we will continually and dynamically evaluate our decisions and practices with respect to the evolving nature of the social contexts we work in; thus, they are not set in stone but are responsive. Taking special security precautions means, ironically, that research

about the importance of context cannot actually include the granular details of study contexts. We believe that such practices are important to pilot and test out, and to err on the side of caution.

In view of this context, the methodological framework has based its analysis on the theory of change which substitutes the 'cause-effect' evidence with evidence that demonstrates 'causal pathways'. To build these causal pathways it uses 'triangulation' which consist in different types of evidence reflecting participants perspectives which are acquired through different data collection methods.

The theory of change requires a framework (or intervention strategy) that shows a clear chain of linked steps between the problems and challenges the intervention wants to tackle, and the expected effect the intervention will have on that problem. It intends to show the links between the project's objectives, the activities and the resources carried out, the outputs that result from these, the short-term results (outcomes) associated with using these outputs and the longer term effects (impact) of the intervention at the broader organisational or societal levels. More in detail:

- Outputs will refer to activities that can be measured in physical or monetary units (number of trips, training activities, people trained, new users of linux or mail encryption).
- Short term outcomes will be defined as indicators that relate to the direct and immediate effect on direct participants brought about the project (increased self confidence, new networks and partners, organisation of a privacy awareness activity, ability to plan and deliver a digital security training).
- Mid and long term outcomes provide information on changes to for example the behavior, or social practices, the capacity or performance of beneficiaries (shifting activism or professional responsibilities, creating sustainable networks over time) .
- Impact indicators will refer to the consequences and broader and longer term social changes of the programme beyond the immediate effects (reducing

online violence, increased technical capacity and know how among communities, better resilience to privacy and security attacks).

Because including gender into privacy and security is still recent and experimental, its deployment remains mostly embryonic or non existent in many areas of the world. This translates into fragmented and scattered fields of knowledge regarding these dimensions. Available, comparable and longitudinal data about women's access, use and uptake of ICT and tech related fields, inasmuch as data about gender-based online violence taking place is largely nonexistent. Accordingly, there are many knowledge gaps in these fields that make it difficult to assess the broader and longer term social changes achieved thanks to interventions, such as this project for instance.

At this stage, only the outputs and short terms outcomes could be assessed. Nonetheless the prolongation of the project in the next three years should enable the design and implementation of new forms of follow-up and data collection methods that could shed some light on the mid and long term outcomes.

Finally, some cautionary remarks regarding our methodology need also to be taken into account. Assessing impact through the theory of change involves focusing on the 'distance traveled' by participants to the project. This distance is linked to the evaluation of hard skills generally clear cut and easy to determine as finding a job, getting a diploma or learning to use a new privacy tool, and soft skills which are often more difficult to collect and evaluate, such as for instance interpersonal skills or self confidence. Besides, analysing the progress participants have made in relation to their anticipated end result requires us to understand their previous trajectory and to create mechanisms that enable exchanges over time. Because of this, communication needs to happen as soon as possible. These regular exchanges and sharing of useful information, even if more time and resource consuming, are both key for enabling participants to travel the distance in relation to their learning needs.

Besides that, because social interventions involve too many dimensions and

complex social realities they can not be easily codified and compared, it is difficult therefore to clearly determine how much or in which precise ways the GTI, and other related training activities, have been a direct inspiration and enabler for the following 50 activities organized on the ground[18]. The fact that most of the selected participants had already demonstrated in their applications a strong trajectory in gender social justice, activism, advocacy, tech development and/or training provision for instance, also explains the amount of activities developed over the past six months.

However, in regard to their use of privacy and digital security tools we found that before the GTI, two thirds of participant had no practical experience at all or only a very basic use of those tools. Since then many participants have incorporated privacy and digital security dimensions into their work much more than they used to do. Distances traveled in relation to these new practices indicate a causal pathway between the intervention and participants effective gaining of new skills and interest for those issues.

Accordingly, the methodological approach underpinning this research comprises several components, unfolding in a relatively sequential form, comprises of the following data gathering:

- Before entering the project: Life trajectories of participants in relation to ICT (access, uses, needs and desires), and more precisely privacy and security tools and practices.
- After entering the project: New skills gained and dimensions in which they are playing out. How their work and activism are being impacted?
- After entering the project: What are the characteristics of the initiatives that participants have then organising on the ground?

While in the last question we will describe gender and tech, privacy and digital security activities that participants have organised themselves or in

18 This report has only analysed 50 activities developed between January 2015 and July 2015. However the repository is now bigger and will keep evolving in the next years: https://gendersec.tacticaltech.org/wiki/index.php/Category:Activities

partnership with Tactical Tech, in the first two questions we will asses more at an individual level what the distances traveled are and the main triggers for change. The next part of this study presents the data collected through the project.

Life trajectories and distances traveled are informed on a statistical and qualitative analysis of two online surveys and discourse analysis among twelve interviews. The surveys were conducted before the GTI (November 2014) and seven months after (June 2015) and dealt with participants expertise and skills, their main learning needs and outcomes. The first survey was answered by 40 respondents and the second one by 32 respondents. Among them 22 answered to both surveys.

The twelve interviews where conducted with GTI participants residing in Africa (3), South America (3), Asia (3) and Macedonia and Turkey (1 each). Each interview lasted between 15 and 45 minutes maximum. In order to complete this analysis, some additional review of storytelling shared by participants and mailing list exchanges has also been conducted.

The second part details the type of collective actions they have been achieving on the ground. The activities' analysis is based on the monitoring and documentation effort achieved by Tactical tech and GTI participants in relation to the initiatives they have organized around gender and tech, privacy and digital security. This also involved filling out a detailed on line form and a review of the press and media coverage of those activities.

Online surveys analysis

As explained above, before the GTI took place, participants filled an online survey in order to provide more details about their use and practices with ICT and privacy and DS tools. It also addressed skills and knowledge in relation to gender social justice, free software, training skills and production of documentation and knowledge. A preliminary analysis of the 40 respondents was achieved in order to prepare the agenda, learning sessions and curricula

to be used during the GTI.

Seven months after the first survey, a second one was sent to all GTI participants maintaining some of the previous questions for comparison and adding new ones regarding current practices and GTI impact. It was answered this time by 32 respondents among which 22 had also responded to the survey conducted in November 2014. We detail below the main changes and impact in relation to the use of privacy and digital security tools, but also in relation to the participants' conceptual understanding of those technologies.

ICT use

The sample of answers indicates that almost all of them use a mobile phone for professional or activist activities. Besides, they all had access to a computer or laptop. There is an intensive use of mobiles devices for work and activism, however the use of end to end encryption services and apps for mobile remains less widespread. This situation stresses the need to develop more specific curricula and related training activities for addressing mobile-specific privacy and security concerns.

On the other hand, 25 of the 32 respondents use free software or open source operative systems, such as GNU/Linux (18) and Android (7). The proportion of participants using different types of OS and more concretely operative systems based on free software has significantly increased with an additional 17 participants claiming to use this after the GTI.

The participants use of free software and open source indicates a willingness to engage with technologies considered by the privacy and security communities as more secure, and liberating as they are based on the four freedoms that grant anybody the rights to access, copy, share and improve those technologies. Besides, from a gender based perspective, engaging with free software makes a lot of sense as this underlines a need to understand how systems works (gender codes, software codes) and how they can be hacked for gender social justice and technology driving social change.

All respondents use social media however the frequency and purpose in their use varies. More of the half states they use them often or all the time. The other half only sporadically or never. Some use it in a low profile, lurker mode and others for actively gaining visibility and becoming a vocal voice in their field. Some use them also for communicating and coordinating with their networks and target audience and others only for making visible their actions but not for internal communication.

Twitter, Facebook and Youtube still rank as the most used platforms. Other social media platforms which have been referred to are Instagram, Tumblr, Pinterest, Google+ and LinkedIn. Interesting to note the presence of only one free and non commercial platform (Diaspora). This suggest that more information about which are current free and alternative social networking platforms available could be highlighted in next curricula.

The intensive and almost pernicious obligation to use those platforms pushed the need for more knowledge about how to engage with those and provide advice others how to best do it in their own context. Because many gender-based online violence happens on social media and because many platforms are not (yet) clearly developing policies that tackle harassment, hate speech and misogyny taking place in their services, many participants felt the need for more tools and methodologies.

Privacy and Digital security

Currently, all the members subscribed to the GTI mailing list use non comercial mails, thereby reducing their potential exposure to massive surveillance, tracking and potential privacy loss. Consequently, all the respondents to the survey used at least one secure mail either on their organisation's mail, or in an alternative mail provider. Augmentation of secure mails is caused by the introduction of participants to mail alternatives and distribution of invites to open up their new email in services such as Riseup and Autistici. So far they

generally keep using those secure mails to communicate with Tactical Tech.

32 respondents use Gnu Privacy Guard (GPG) for encrypting their emails. 20 of them began to use it before the GTI and 12 began to use it after the GTI. Nonetheless it can be remarked that 19 of the respondents stated that they gained confidence using GPG thanks to the hands on sessions delivered during the GTI. Another factor was that they could also practice its use by communicating with other participants using encryption. Again it can be noted that digital security is a collective game in whichyou need others to engage with you in safer communication practices and this requires not only using similar tools but also knowing how to use them adequately.

The survey asked participants if they understood the following 5 concepts: How the Internet works ; SSL Digital Certificates; How viruses and malware are transmitted; Http:// Vs. Https://; Free software Vs. Proprietary software. More than two third of respondents claimed to understand all concepts and the other third understood between 3 and 4 concepts. In comparison, before the GTI less than one quarter of participants understood all concepts, while more than one third of respondents only understood one or two concepts. Those figures shows that participants have gained understanding around the basic principles guiding the architecture of Internet and digital security.

Understanding of concepts	November 2014	June 2015
Understood all concepts	23%	72%
Understood between 3 and 4 concepts	40%	28%
Understood 1 or 2 concepts	38%	%
Privacy		
Use a free software or open source operative system	20%	78%
Use an alternative secure email	NA	100%
Use GPG for encrypting their emails	NA	100%
Gained confidence using GPG during the GTI	NA	59%
Became more confident in privacy advocacy	NA	72%

Table 1: Comparison results November 2014 - June 2015

More than two third of respondents claim that they've become more confident in privacy advocacy, and are more convincing about why privacy matters and

how to trace one's digital shadow. More than half of the respondents have also become more confident with managing various online identities, countering the nothing to hide argument and adapting privacy settings in social media profiles. Understanding data mining and data brokering have been the categories less selected indicating that more curricula and adapted training is needed in order to understand who is collecting, selling and using our data for profiling or tracking us. In relation to a more confident and systematical use of privacy and digital security tools, we can also see significant changes between the two surveys.

As introduced previously, mail encryption is now practiced in a most self confident way many respondents achieving impact in strengthening the web of trust among WHRD and women activists. Besides that, nearly all participants (31 out of 32) use strong passwords. Interestingly enough we found a similar percentage in the survey achieved before the GTI but afterwards receiving training many participants acknowledge that their passwords were not as strong as they thought.

Far more participants clean and back up files, encrypt mails or devices, and use anonymisation tools. Less widespread digital security practices, such as the use of Virtual Private Networks and tools such as the Amnesic Incognito Live System (TAILS) are now used by about 40% of respondents. Those tools show the highest increase as only 10% of respondents used them before attending the GTI. To note that almost all respondents have also started to gain confidence in more than four types of tools and practices increasing their capacity to protect their data and engage in safer communications online.

Overall, a large majority of respondents (29 of 32) found that the GTI contributed to a better understanding of the interaction between gender and tech, and enabled them to count with an enlarged network of support and friendship with other women engaged in gender and social justice that share an interest on privacy and security issues. The same majority also underlined the impact the training track session had had in their self confidence and better understanding of digital security and privacy trainings development.

Which of the following digital security practices do you apply?	November 2014	June 2015
Strong passwords	98%	97%
Cleaning/back ups files	68%	88%
Mail Encryption	43%	94%
files/devices Encryption	38%	59%
Chat/VOIP Encryption	25%	78%
Anonymisation	15%	53%
VPN	15%	47%
TAILS	8%	41%

Table 2: Comparison results November 2014 - June 2015

Interviews analysis

"GTI changed my life. My life turned around" (JA)
"It has been like a big spring of inspiration" (NR)

The following profiles of participants interviewed include both WHRD who discovered privacy and digital security at the GTI and women already involved in gender and tech activism. Some work in established NGOs meanwhile others contribute to activist groups and informal groups often as volunteers. Some of them engage in both ways. The interviews have focused on their relationship with technology and how they have accessed and are using it, their perceptions of gender issues in their life and in relation to tech, the impact of the GTI and their desires for the future.

Interviewee /Geographical origin	Work /Activism
M. Y - Egypt	LGBTQI rights organisation
Y. O – Kenya	Women's rights organisation addressing violence against women
P.L – Democratic Republic of Congo	ICT project manager for Women's rights organisation addressing violence against women.
G.D – Nicaragua	Organisation promoting woman involvement in technology and WHRDs using technology to defend rights
F.S – Brasil	Digital Security trainer
J.C – Mexico	Collective of social change advocating for free software
T. A– Argentina	Hacklab promoting free software and free culture

D. C – Indonesia	NGO using technology to push for environmental justice digital rights, gender and sexuality issues
R. S - Cambodia	Organisation defending civil rights and freedom of expression
N. R - India	Organisation working on displacement issues
J. A– Macedonia	LGBTI rights
I. M – Turkey	Organisation focusing on digital rights and privacy

Gender and tech : Connecting the dots

All interviewees remarked that their gender played a role in their access to technology, whether in their family, at school or university, or in the work place. In most cases, their first memory of technology consisted in devices they borrowed from their familiars, brothers or parents. Many underlined that in their contexts, girls were not encouraged to use and learn about computers or ICT in general.

"My gender did not allow me access to technology or internet. People do not think about what kind of technology is used by men, what kind by women. You don't see it clearly, but the barrier is there" (R.S)

"Maybe I did not think I was supposed to have a computer but my brothers had a computer right away, so I just used theirs" (F.S)

This limited and often controlled access to technologies also prevented them from feeling legitimate in those fields, even when studying computer sciences, or when becoming advanced users through self-learning and trial-error practices. From early childhood to first professional occupations, all of them underlined how cultural and social gender beliefs associated computers and ICT with inherently masculine occupations. Those who grew up with good

access to technologies, or did specialise early in technological jobs also acknowledge that they were not fully conscious until recently of the impact of gender on their access, use, and uptake of technologies. Many had internalised the gender gaps that prevented them from advancing further on.

" I remember once I went to a job interview, about a topic I knew well although I was young; I had been doing that for already 4 years and the guy told me I was too nice to be there, that I should not do that, that it was a man's job » (F.S)

"Now I'm seeing it better than before, I was not serious about knowing more about technology because of the prejudice of being a women. I was not aware of how much I could accomplish" (J.A)

"Of course, there was a presumption that it's something that's hard and not my cup of tea, although I was interested in it, there was a subtext that I should do something in the humanities field, not take things apart and study computers" (R.S)

The GTI acted as an eye opener about the relation that gender played in relation to technologies. By comparing trajectories and common challenges, and presenting initiatives for reducing the gender gaps in STEM and Computer Sciences, but also feminists perspectives of technology permitted participants to better grasp the different inter-relations linking gender and tech. It could also be seen that this increased consciousness has given many interviewees the desire to start collective actions and change things. They want to develop more gender equity and social justice in tech related environments.

"Even if I was in the techie world I did not have much concepts, notions about gender and tech [...] The GTI showed me the feminist approaches to tech, and that was really good" (F.S)

"Before I trained on digital security I used to train on ICT tools and now getting the gender perspective to ICT tools, that's phenomenal for me" (Y.O)

"I think there is a very big problem of gender gap in the technological field. After the camp I read a lot more about it, now I know that it is a systemic thing and not just a vague discouragement that I have faced. It is a problem that needs to be fixed" (N.R)

"I have met so many women who have gone through cyber bullying and seen the impacts that it has had on their lives. For me training on privacy advocacy and digital security is more than just training it is about sharing critical information that will change the lives of women in online spaces" (Y.R)

Figure 4: A poster of an activity organised by a GTI participant

Breaking the circle of isolation

"It is a gift that keeps on giving" (N.R)

Many interviewees have acquired their technological competencies in a self taught way and had a desire to learn more that could not be satisfied through their local networks, in particular because of the lack of other women and allies involved on those topics, lack of safe spaces and/or because of the prejudices they felt against women being involved in technologies. Because of these reasons, many interviewees experienced relative states of isolation in relation to their practices with ICT and expressed strong needs and feelings about exchanging with peers and counting with a network of exchange and support.

For many interviewees, the GTI enabled them to learn more in a collective way (everyone learn from everyone), build a network (Do It With Others) and feel legitimate (I am not alone).

"I'm really grateful I was in the space, not only learning from facilitators but from other participants" (D.C)

"I met incredible people, it helped me build a network that is not project specific but important in terms of help [...] It helps to know people somewhere else in the world who do the same things at the same time" (N.R)

Interviews underlined how this encounter and contact with peers from all over the world constituted a relief and an input of energy and creativity in their work and activism. The realisation of the active and multifaceted contribution of women to tech and privacy and digital security had also an impact on existing imaginaries enabling new role models and mentoring opportunities.

"When I knew about the GTI I was really exited about it cause I felt very alone in what I did, even if I knew other girls that were into digital security, they were not working with activists and in the end I felt like the only women" (F.S)

“I wasn't aware that there are so many people, women working on the project, so dedicated and amazing, that was one of my favorite things to realize in the GTI” (J.A)

Most of the people interviewed pointed out the need to improve their local networks. In order to disseminate the knowledge they acquired, open new perspectives and collaborations, more initiatives need to be supported on the ground. In relation to that, it can be noted that six local activities were organised among GTI participants who did not know each other before. Subsequently, we believe that the next regional GTI should further support this dynamic of creating local networks and breaking the isolation of women engaging in those fields.

“Some of the things we might need to continue doing our work better and stronger is local support. I've had a lot of meetings with local groups which are working also around DST, but the issue for our collaboration is to get funding” (G.M)

“We have the will to build something, like the hacklab for instance, we want a space that women, non binary and trans can come in. A GTI in Brazil would help to achieve those objectives” (F.S)

Figure 5: A digital security training for feminists organised by a GTI participant

Advocacy and Training skills

The GTI was designed to increase the technical capacities, self confidence and networking skills among WHRD working around the world in order to enable their inclusion in the privacy and digital security fields. It included two specific track sessions to improve participants training and privacy advocacy skills. It also build upon the wide variety of expertise brought in by Tactical Tech and APC, as well as the skills participants brought to the GTI. Put together, this transformed the GTI into a multidimensional training hub.

Many interviewees felt they had become more confident with drafting a training cycle, developing risk assessments and threat modeling, which were topics they had not been so much exposed to before. Adult learning methods, such as the ADIDS inasmuch as exposure to new types of feedback and evaluation methods were also felt to be very useful. Besides that, many underlined how the holistic security perspective benefited them and more precisely enhanced their capacity to engage with WHRD and women activists within trainings. The fact that we did not only focus on digital security as a set of tools, but as a set of methods for creating a general atmosphere of safety, self care and psychosocial wellbeing was seen by the participants as a great enrichment of their capacities.

"The whole process of facilitating, the methodology used was very nice. I try to do the same. It was a very holistic experience, I really like it" (J.C)

"What was very useful was the approach, the meta knowledge: the way to do the trainings" (T.A)

"My skills as a trainer are a result of the GTI, I have the confidence that I can be a trainer here locally so I can do something more about it." (J.A)

"When I attended the GTI, I went with one mission - to identify new areas of privacy advocacy and digital security that I could adapt as I continue my work in training and facilitating roundtable discussions in the future, as I seek to

reach out to different target groups of participants. Here the idea of flash trainings and being innovative with how we advocate for security skills was sharpened. I also learned new digital security tools that I could share that are in line with the changing times" (Y.R)

The first part of this analysis has presented the main outputs and short term outcomes gained by the participants to the GTI through an analysis of their life trajectory in relation to ICT and the distance traveled in relation to learning new technical, training and social skills. The next part will address the collective dimension of those processes by analyzing the type of activities organized on the ground and which type of aims have been addressed, audiences reached and topics addressed. The analysis is composed of a statistical review of the 50 activities, followed by a more in-depth presentation of some specific initiatives.

Collective actions and networks
Activities around gender, privacy and digital security

"During several days I felt shaken by the experience as it felt that this workshop was completely different, not only because I achieved technical things that I had not done before, but above all because there was an atmosphere of hope, but not of false hope, it was the hope that comes from knowing that you can do things, that we could move from fear to self-defense and that we could move from doing it alone to do it together" (M.S)

The following section presents an analysis of the 50 activities organised on the ground by GTI participants between January and July 2015.[19] There have been relevant experiences and initiatives dealing with gender and tech, privacy and/or digital security for raising awareness or skills sharing and addressing end users, intermediary actors and/or organisations. In order to operationalise our research we refer in this document to the above analysis with the terms initiatives or activities. Those terms are defined as collective actions involving

19 This report has only analysed 50 activities developed between January 2015 and July 2015. However the repository is now bigger and will keep evolving in the next years: https://gendersec.tacticaltech.org/wiki/index.php/Category:Activities

strategies intended to resolve difficulties and/or improve a situation in relation to access, use and uptake of privacy and digital security tools and practices.

All those activities have been organised either directly by the participants to the GTI (alone or in partnership with their organisations and communities), or by Tactical Tech with the involvement of different GTI participants.

In order to document those activities, the methodology has consisted in a follow up achieved through personal emails, mails exchanged on the GTI mailing list and also face to face meetings during events where we could receive direct feedback from the participants. We have been keeping track of those exchanges and, once our on line resource space was available, created a template for each recorded activity. We also created an editor account for participants and invited them to further document their initiatives. Besides that, all the others GTI participants that did not report an activity were also invited to request an editor account in case they wanted to share about their work and contribute to collective documentation.

This sample of activities should be understood as a snapshot of a specific panorama taken at a given moment and not as a representative image of the current state of the art in relation to the development of activities around privacy and digital security including a gender approach. Some evidence about other activities could be found on the qualitative interviews and the answers to the survey. However because they were not directly and actively reported through the channels detailed above, we did not include them in our analysis.

Furthermore, some activities documented in the wiki have been left out of this analysis, such as the TransHackFeminist convergence[20] (Mexico) that took place at the end of July and which documentation was still not available at time of writing this report. Activities organised only by facilitators of the GTI, and not involving directly any GTI participants were also left out of the sample as for instance, the 'Zero Trollerance campaign[21]' or the panel for including gender at

20 http://transhackfeminist.noblogs.org/
21 http://zerotrollerance.guru/

the Re-publica conference[22]. However all of them can be found in the wiki as their documentation provides interesting insights and adds to the reservoir of inspiration for organising more activities of that type on the ground.

Other limitations constraining our analysis relate to our commitment to the do not harm principle. As introduced previously, our experience in the field indicates that the lack of feedback and documentation can also be strategic from a safety and wellbeing perspective. On the one hand we find that a large amount of activities are based on volunteer work, which generally does not allow a proper planning, documentation, and analysis of its outcomes. Precarious living conditions of many participants generally comes with a lack of time and resources to develop documentation processes.

Besides that, documentation in the context of our target audiences requires us toachieve a balance between the political and inclusive potential linked to our documentation processes (sharing is caring) and the visibility issues that can expose participants to threats or repression (sharing is scaring). As we looked for ways of creating safe spaces online and offline, where we could create a sense of community and self support, we were pushed towards the need to create missing resources that could be useful to our specific communities needs and challenges. By documenting what we do, why we do it, for and with whom we are doing it and what the outcomes of those collective actions are, we are easing the process for others that might want to engage in those fields but still lack references, networks or experiences.

However, as many participants experiment a lack of privacy, are under surveillance or live in highly controlled and monitored environments, how they share information and how they present themselves can result in unexpected outcomes at best, or more threats and repression at worst. The project intended to think ahead of those challenges by training participants to understand how they should ponder visibility with traceability and exposure

22 https://re-publica.de/session/including-gender-new-approaches-privacy-and-digital-security

before publishing online. More concretely, our invitation to document included a memo recalling participants that before documenting on the wiki, they had to carefully think about what they published could affect themselves and others.

In addition, only six fields of our template form were compulsory in order to record an activity. Namely its title, category (gender and tech, privacy and/or digital security), date, target audience and the number of people trained. Those criteria were retained because they could give a sense of the activity without revealing the actors and organisations behind it. However many activities could be documented in a far more detailed manner including useful information such as agenda, tutorials and learning resources, participants feed back, learning outcomes and thoughts for the future.

Through our exchanges with participants and our review of available platforms and on line resources for learning more about privacy and digital security, we were able to identify a gap in relation to available Open Educational Resources encompassing more immediate privacy and digital security resources for trainings. For instance, many learning opportunities can arise from a well-organised and searchable repository of agendas. By reviewing how different agendas can fit specific audiences and time constraints, trainers and advocates can improve their own planning. In the same sense, presentations that can edited and adapted to one's context can ease the process of preparing useful training contents. As we could see through the project, many new privacy advocates and/or DST that are working on a volunteer basis will struggle with time and will experience difficulties in fitting new training and advocacy activities into their already busy lives. Because of these constraints, platforms that share proper documentation can enable a better access for all to learning resources. These different considerations brought us to develop a wiki, which is one of the most comprehensive and widely used platforms to create community driven documentation.

Geographic scope

As said on introduction, the impossibility to document all the ground-based

work resulted in a sample of activities documented through direct feed back from their organisers. Nonetheless we were also able to spot evidence of other activities taking place in the Asian, sub Saharan and MENA regions. Many of those activities were not reported or published as the organisers wanted to "remain under the radar."

So far, almost half of the activities reported on have taken place in Central and South America (24). Countries covered were Mexico (9), Brasil (7), Argentina (4), Guatemala and Nicaragua (2 each). This over-representation should also be linked to the background and experiences of the GTI participants among which many were already involved free culture and/or free software collectives. Within these types of tech communities, documenting practices often lies at the core of their sustainability, this can partially explain the over representation of this region in our sample.

The second most active region was Asia (11) encompassing activities in the following countries: Cambodia (3), Pakistan (3), Myanmar (3) and India and Indonesia (1 each). Regarding the African region, all the reported activities (4) took place in Kenya. And for other countries, we found an activity organised in Serbia, Macedonia and Turkey. Finally, some activities were also organised in the UK (2), Germany (1), Czech republic (1) and Spain (4) during the Circumvention Tech Festival[23], an international event in the digital security field. To note that some of those events also targeted audiences from the global South.

Even if the following distribution of activities can not be taken as fully representative of the current environment, it indicates however that there is a need for pushing more partnerships and collaborations with current and future participants to the GTI in the sub Saharan, MENA, and post soviet regions.

23 https://openitp.org/festival/circumvention-tech-festival.html

Objectives and formats

The main aims motivating the organisation of the activities are divided between:

- Privacy Advocacy Activities (8) which generally consist of sessions designed to raise awareness, discuss and better understand privacy implications driven by our uses of technologies. They can address specific national legislation, how to deal with surveillance and interception, corporations practices with data mining and profiling, new forms of surveillance and control exercised by private actors. The activities generally last less than one day and consist of workshops, panels, talks and screenings for instance.
- Digital Security Trainings (34) which generally implies sessions designed to raise awareness on digital security practices and better understanding through hands-on activities on how to find, use and configure digital security and privacy tools. Those trainings generally last from half a day to three days or more. They can also be provided from an holistic perspective or consist in train of trainers (ToT). We have ranked those sub-types of DST below.
- Holistic security (5) refers to specific trainings and workshops delivered on the ground with a holistic perspective, which enable trainers to link physical integrity, self care and wellbeing along with digital security practices.
- Training of Trainers (3) refers to specific activities that are aimed at training persons already engaged in delivering training on any of the topics listed above in order to increase and/or update their training skills.

Please note that these global categories can easily overlap and that boundaries are fluid in practice. We saw that many participants when developing activities address privacy along with digital security. The tensions

existing between those dimensions in relation to the availability of tools, the possibility to own your tools and processes, threat modeling and risk analysis differs greatly but many GTI participants addressed both dimensions at the same time in the activities they developed.

Besides, the objectives of an activity, we also find the type of formats that are chosen to achieve it and which can adopt different shapes. Because a clear description of the format was not systematically provided, many activities have fallen in the generic "workshop" category (28) which includes any session involving a hands-on aspect with privacy and DS tools. However the remaining formats such as talks (7), panels (4), hackathons (4), cryptoparties (2), 1 to 1 (2), barcamps, screenings and edit-a-thons (1 each), reflect possible collective actions for reaching out to various audiences. Besides, formats such as hackathons, cryptoparties, barcamps and edit-a-thons refer to practices developed in the FOSS and digital security fields showing how GTI participants are actively contributing to those worlds.

Most of the activities (35) were not open to anyone. Attendance was largely on a personal peer to peer invitation or promotion through trusted networks, on line registering or through selection processes. These closed calls were often related to activities targeting women and LGTBQI in controlled and/or hostile environments. As providing training to digital security, privacy advocacy or gender and tech is considered in many contexts highly sensitive, it can require that organisers keep a low profile to avoid attracting unintended attention by opponents. The remaining activities were open events (15) aiming in general to raise awareness and/or train specific audiences, generally without limiting participation to a specific gender or sexual orientation.

We have broadly classified the activities between those that lasted less than one day (35) and which generally encompassed PA activities, talks, panels, screenings and in general any type of flash trainings. However there has also been a significant amount of activities lasting more than one day (13), generally two or three days and consisted of training of trainers and in-depth digital security training for specific audiences, such as journalists or activists

(anti mining, environmentalists, social gender justice, LGTBQI rights). It is noteworthy that in general the longer trainings received some type of funding from the organisations enabling their sustainability. On the other hand, many activities lasting less than one day were based on voluntary work or in house trainings provided by GTI participants to their own organisation.

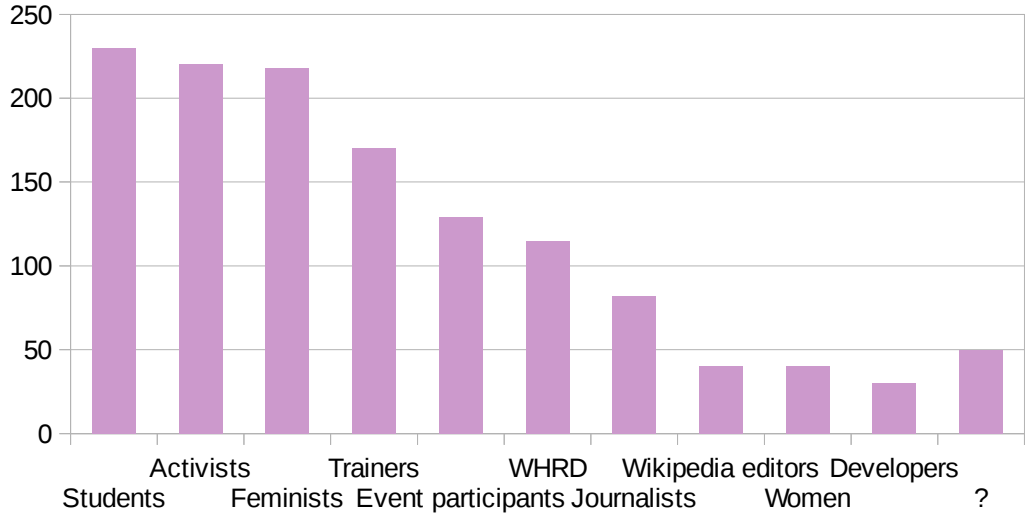
Figure 6: Project coordinated by one GTI participant

Out Reach

Classifying audiences under an unambiguous banner can prove as tricky as precisely naming formats. Many activities included in their call a multi-layered description of their target audience such as for instance "open to activists, feminists, LGTBQI". For the purpose of this assessment we have labeled each activity under a main target audience with the following clusters: Activists (12), Feminists (8), Participants to events (7), Woman Rights Defenders (6), Journalists (5), Students (3), Trainers (3), Women (2), Wikipedia editors and developers (1 each).

As the number of participants was compulsory for recording an activity, we can see that all together the 50 activities reached 1324 persons. If we detail the

amount of persons reached in relation to the type of audience we found the following : Students (230) that encompass largely women students in countries such as Pakistan and Kenya, Activists (220) as a more generic cluster encompassing different areas, and Feminists (218) which includes feminist collectives around the world. The main target audiences are followed by Trainers (218) largely attending Training of Trainers activities, participants to events (129) such as the Circumvention Tech Festival and big Crytoparties, and Woman Human Rights Defenders (115). Finally, journalists (82), wikipedia editors (40) and developers (30) at the edit-a-thon and the hackathon activities were also reached.



Graph 1: Cluster of publics reached out through activities

As explained previously many activities were upon invitation only and could targeted specific gender identities and/or sexual orientation. Most activities were oriented towards mixed environments welcoming all genders (24), and the rest required participants to self identify as a woman (19) and/or as a LGTBQIA (6). If we add up the number of people trained according to their gender and/or sexual orientation stated on the call for the activities, we found that woman (538) are the main target, mixed environments (593) (also including women) account for the second place, finally followed by LGTBQIA (153).

This high number indicates that investing on training skills of WHRD and women net activists has a multiplier effect proving our methodology for reaching out to vocal woman and social change makers who can act as intermediaries within their own networks. We can identify a clear causal pathway that links the trainings achieved under this project, and a clear social return at the level of the communities and organisations that trained women are engaging with.

Even though an analysis of the outcomes of each one of those 50 activities can not be achieved here, we found that many participants when reporting feedback from the participants that attended their activities wanted to learn and engage more, reach more participants, create more similar activities and/or scale them up. Besides that we can also see that for the GTI participants, developing these activities helped them boost their confidence in their knowledge and skills and introduced them to new social networks for further engagement.

These are very positive indicators and the organisation of the next regional GTI events will further contribute to breaking the isolation of GTI participants and grow more networks of support and trust expertise at the community based levels. The table below present some extracts regarding the feedback from GTI participants who organised activities as well as some of the feedback they received from their participants.

GTI participants feelings	Feed back of participants to activities
Loved sharing my knowledge on digital security but above all, loved the attendees enthusiasm on the subject matter. When the training came to an end, the participants were not willing to leave the training session. Their silence was pregnant with the desire to learn more. This filled me with lots of joy to know that we had been tackling a topic that people	The participants found the sessions useful not only in their professional lives but also in their personal and academic life. The sessions were structured to be as responsive to the developing needs of the participants and there was open interaction towards finding practical solutions even beyond the training days. One participant remarked- " It is like I attended a

are hungry for information. It was a reflection that probably it was interesting and relevant to their day to day work. (Kenya)	full course." At the end of the training participants committed to being part of the driving force at the association on matters tech, gender, security and advocacy. (Kenya)
Then unexpectedly I got an encrypted mail (:P) proposing me to join a facilitators team and do my first training as a co-facilitator. First I got scared and wasn't sure if I knew enough, as I was still learning and it is a great responsibility talking about security. I had the opportunity to share my modest knowledge but also be part of a DST team, so I realized that it is a great challenge that I can't miss. Luckily I didn't have to "invent the wheel" again and I was using the resources that other DS trainers have already put online to help people like me. In the same time my creativity was also challenged so it was a very interesting process. (Macedonia)	It was one of the best trainings i have ever attended!!! Facilitation was perfect. I liked that there were three facilitators and topics were shared. (Balkans) The training was very interesting. It created a lot of possibilities to me to know what are the options for secure online communication. Facilitators were very attentive and great. (Balkans)
As the organizer, I felt a great satisfaction to be able to conduct the training and share what I have learned in the past year. This small achievement serves as a seed of work to show and convince activists about the importance of the issues and it also serves very valuable ground work for me on the issues to build the gender and tech movement in Indonesia. (Indonesia)	Participants were very grateful and excited about the event and the new issues they were learning in the training. All of them were very excited to share what they have learned with their friends in their organizations and collectives as now they know that most of digital security strategies will only work if it is applied collectively. Participants also express their hopes for the continuation of the training and discussion after the event, not only for women and LGBTIQ activists but also for other activists working on different social justice issues. (Indonesia)
It was extraordinary. I felt like a pioneer who started a completely new topic related to the conquest and preservation of women's human rights. Right to IT security and privacy. (Serbia)	Great interest of the participants and the desire for more knowledge in these areas. When it comes Younger participants, they have a decent technical knowledge, but lack awareness of the risk and responsibility. When

	it comes to older participants, among them was noticed ignorance ways of functioning of the Internet and the dangers that hide behind that, though they include it in their daily lives, both business as well as private. (Serbia)

Figure 7: One activity organised by a GTI participant

Organisations

Most of the activities (36) have been pushed by organisations, in general the ones that GTI participants are working with or for. It should be also noted that a portion of the activities were organised by organisations for its members only using formats, such as in house flash trainings, talks and also more advanced digital security trainings. Nonetheless, there is also a significant amount of activities (11) which were organised by individuals. In some cases participants are keeping their activities as privacy advocates or digital security trainers separate from their work or other types of activism. It is also interesting to note that among those eleven activities, we find that six of them were developed through a partnership between different participants of the GTI. This was made possible through the new connections they gained by attending the

GTI, which became new contacts in their field. In terms of the full sample it can be also noted that twelve different activities brought together more than one GTI participant enabling new encounters and networking over time. We believe this is very interesting for breaking the circle of isolation felt by participants and we believe that the next regionals GTI will enable to make further progress on that strategic line of action.

Regarding Tactical Tech's contribution, the detail of activities shows that it has played an active role in supporting 18 activities. It acted as a facilitator for the direct organisation of two activities, enabled new training opportunities for twelve GTI participants through six activities which encompass three train of trainers and three direct training to woman human rights defenders activists. Besides that Tactical Tech used its outreach budget to fund nine activities delivered under the Femhack world initiative and one initiative for training women in Pakistan.

Moreover there is a record of 17 activities organised by GTI participants which used Tactical Tech self learning materials. These include the Women Rights Info Activism Toolkit[24], the community focus guide Security in a Box for LGBTI in the MENA[25] and sub-Saharan regions, Me and My Shadow[26], and Security in a Box[27] were used for trainings and/or distributed by organisers. Incidentally, whilst we were gathering feedback in the in-depth interviews, interviewees underlined frequently the need for more printed materials, more translations and more materials that are not mainly text based but include visualisations, infographics, audiovisuals such as podcasts and videos for instance. After this presentation of general characteristics of the activities delivered on the ground, we detail a selection of them below in order to better understand their outstanding heterogeneity, creativity and outcomes.

24 https://womensrights.informationactivism.org/
25 https://securityinabox.org/en/lgbti-mena
26 https://myshadow.org/
27 https://securityinabox.org/

Detail of activities

Raising awareness against online misogyny: The Zero Trollerance Campaign

This campaign[28] was inspired by debates and exchanges regarding gender based online violence and trolling that took place during the GTI and were informed by participants experiences. This initiative was designed by a facilitator of the institute in partnership with the Peng collective which is a Berlin based communication group. The initiative was widely supported and relayed by many participants to the GTI. As explained in their website in a humoristic manner: *"Hate has always been a part of the Internet and the intentional harassment of other people (termed trolling) has too. But the gendered forms of harassment and violence on Twitter today point to a deeper problem in society that cannot be solved by technical solutions alone. Trolls need serious, practical help to overcome their sexism, deal with their anger issues and change their behavior".*

The campaign enabled you to send to your Twitter trolls links to individual videos or to the main website. The campaign involved 160 talking bots that enrolled 3,000 identified trolls in the 'self-help program', and then sent them humorous motivational messages and video clips over a period of one week. This initiative received a wide media and press coverage contributing actively in making more visible the problem of gender based online violence and misogyny taking place on social media platforms such as Twitter.

28 http://zerotrollerance.guru/index.php

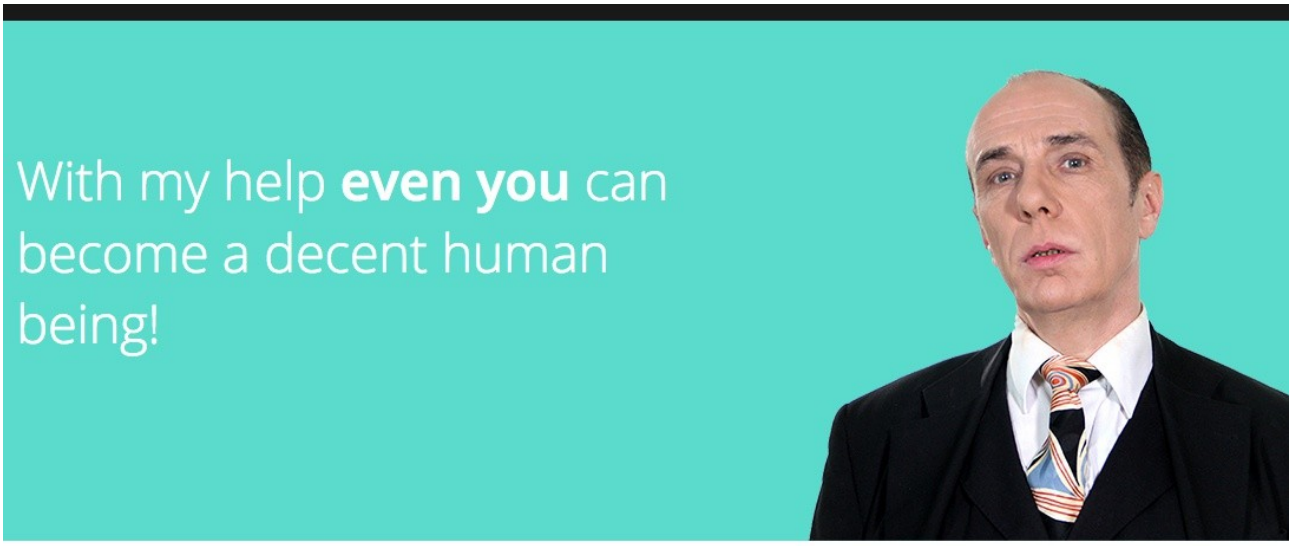


Figure 8: Home page of the zero trollerance website

Raising ICT skills of women in urban and rural areas: Hamara Internet

Hamara Internet is a project developed by the Digital Rights Foundation whose founder and director, attended the GTI. So far, the project has hosted four workshops in different remote towns of Pakistan for around 180 women activists and students, who were trained to use social media and digital tools to make their work more effective and safe. After different sessions they knew about the different laws which deal with cyber abuse and violence and they also learned about the basic digital security tools and privacy techniques they could apply when engaging online. Women reached were mostly from rural areas or university students. Participants reported to have gained confidence to not only actively participate in the online sphere but eventually to transit towards more online forms of activism. For achieving the Hamara Internet Campaign, Digital Rights Foundation has partnered with groups like Tactical Technology Collective, the Web We Want and local groups like Peshawar 2.0 and City University Peshawar.

The initiative also developed a website[29] including digital security content in

29 http://hamarainternet.org

Urdu language from Tactical Technology Collective, information regarding training and workshops, research and advocacy material, and women related laws and policies in relation to cyber abuse. Along the project, materials such as stickers, and badges with different messages about privacy and cyber abuse against women have been widely distributed.

Figures 9 and 10: Pictures taken during Hamara internet workshops

Sustained training over time: The Digital Trainers Summit

As underlined by our in house research report "Security in context"[30], reaping the full benefit of training to privacy and digital security requires support to sustained learning over time. Our experience in the field indicates that participants take advantage of more than one learning experience in order to integrate digital security practices into their groups, organizations, networks workflows. For any type of sustained uptake, one training serves as the basis for learning but a second training provides the space and time to solidify skills, strategise at a movement, network at organisational level, and to support the growth of champions. Participants to those training activities told us that they began to understand the context behind the tools better the second time

30 Publication forthcoming (2016)

around. Because of these elements, in the six months following the GTI, the project enabled 12 women (a quarter of all participants to the GTI) who were interested with opportunities and resources to attend new training opportunities.

These include providing a digital security training aimed at WHRD with more experienced trainers, or it involved attending a Training of Trainers (ToT). Among them one was focused on holistic security and two more focused on digital security. It is in this context that through a partnership with IREX and Internews we were able to invite six participants from the GTI to attend an international event about digital security which included a Digital Trainer Summit. Its objective was to gather a cross-section of the growing community of digital security trainers in order to establish a sense of the community, map their work, and identify commonalities, differences and best practices in the diverse approaches present in the room. The participants were roughly 60 digital security trainers from regions including Latin America, the Middle East and North Africa, sub-Saharan Africa, the former USSR and South-East Asia, among others.

Participants from the GTI shared an evaluation about their experience at this ToT and underlined that it had been a crucial moment for meeting more peers and strengthening their visibility and participation in the field:

"I think the sessions were very fruitful to me to learn about best practices from other trainers, on what I think I can apply in my trainings. We also tried to formulate a way to shift the focus of digital security trainings from tools to humans" (D.C)

Participants also agreed on the importance of training again the recent acquired skills at GTI in order to feel more confident and keep up with their interests on those topics. As explained by one of the participants after delivering a training for WHRD in Mexico that followed up her participation to the Digital Trainers Summit:

"For me, attending the Gender and Technology Institute turned to be a very intense experience and I have to admit that it was not until the Circumvention Tech Festival that I could begin to put a name and give voice to the range of emotions the GTI had caused in me. To be nourished with reflections from such a broad diversity and understanding the holistic security approach served me a lot" (M.S)

Figure 11: Website of the Circumvention Tech Festival

International Feminist Hackaton: F3mHack

The desire for this global feminist hackathon emerged from different individuals that met at the GTI and wanted to cross feminist and post-colonialist perspectives of technology in order to engage with a global network during a 24 hours hackathon. One important aim was to create trans-frontier solidarities in order to break the circle of isolation felt by many participants in relation to those topics. Besides, the idea was also to enable a multilayer of safe spaces (online and offline within the different initiatives organized in the ground) where women, trans* and other interested persons could learn about how to protect their privacy and digital security in feminist, friendly and nurturing environments.

In terms of concrete logistics, a first date was proposed around March but participants were too busy at that time. When Sabeen Mahmud, a WHRD from Pakistan who had organised the first hackathon in that country was shot dead, participants to the femhack mailing list proposed to dedicate the feminist hackathon to her memory and a new date was decided for the 24th of May. Under the umbrella of this international call for action, Tactical Technology Collective funded nine outreach initiatives organised by GTI participants in Mexico, Argentina, Brazil, Indonesia, Kenya, Serbia and Pakistan.

Figure 12: Banner of the FemHack website

It should be clearly underlined that the call for participation, website design, translations were all based on volunteer work, and resulted into a bottom up and decentralized effort among participants who engaged together by using different means such as encrypted mails, protected chats and pads, collective administration of the website. Last not least, even though the public launch of the call for actions could only be issued 2 weeks before 24th of May, 25 new activities were submitted. Added to the eleven organized by GTI participants, the Femhack amounted to 36 activities which lasted between one and four days and were delivered in 19 different countries[31]. In general organizers of those events have been women or LGTBIA persons, but there were also cis men interested in feminism and approaching technologies from a post-colonial

31 Map with detail of activities can be seen here: https://f3mhack.org/index.php/en/

perspective who submitted proposals and developed activities. We detail below some of the activities organised on the ground, listing first the initiatives organized by GTI participants and funded by TTC and adding a selection of other initiatives organized by third actors.

Activities funded by TTC:

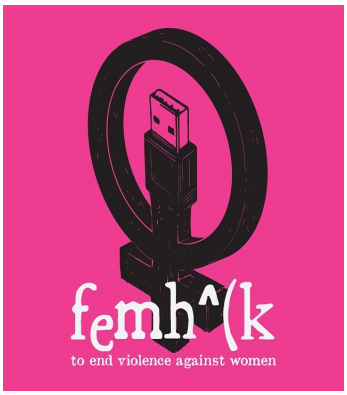
- Argentina: Hackelarre for feminist & LGTBQIA about basic privacy and digital security. It gathered feminist collectives and queer, trans, cis women & women of color from Buenos Aires.
- Brazil: Hackdays for feminists women and LGTBQIA in order to raise awareness on privacy and digital security.
- Mexico: A Feminist Caravan of 1200 km that went to Guadalajara, Distrito Federal, Puebla and Oaxaca in order to make visible risks faced by WHRD and journalists meanwhile providing practical workshops for self defense.
- Mexico: A workshop for WHRD in which digital security departed from an understanding of the basic principles behind internet and how the information travels.
- Serbia: A round table about privacy and security organised by the Association of the Woman Development Center in order to raise awareness about privacy issues currently faced by WHRD.
- Kenya: Talking Digital, Saving Lives was a workshop organized at the Egerton University which addressed issues of tech related violence among students of higher learning institutions.
- India: Encryption and digital security workshop for cis, trans and queer women aim at introducing some useful secure communication practices and tools to help LGBTQI organize among themselves.
- Indonesia: A feminist hackaton and digital security training for women and LGTBQI people.
- Pakistan: Workshops on Safe Spaces in the universities of Islamabad & Lahore where the Digital Rights Foundation introduced to the concept of online and offline spaces and the methodologies that can support their development.

Other activities:

- Global: Take Back the Tech! Hack the sign! from APC was designed to transform the meaning of WiFi symbols turning them into symbols of women amplifying their voices and connecting their ideas. This action used the hashtag #Occupytheinternet! And aimed at challenging patriarchal culture and norms in our relationship with technology.

- Scotland: A queer crypto meeting was hosted and also organised a round table on the political background of the current crypto hype, discuss its relevance for gender issues, and then went hands-on supporting participants in their use of encryption tools.

- Tasmania: Miss Hack hosted a technological coven on the access to technology from the point of view of women and the relationship between creation, information and health, to empower embody and embrace kindred actions in the spirit of Sabeen.



Conclusion

After one year of development of this project, we can confirm that issues of privacy, online security, freedom of opinion and expression and new forms of ICT based violence and online misogyny are certainly shifting and expanding as the online space matures and more women activists and WHRD come online and begin to tactically use ICT for strengthening their work and activism. Phenomena such as online harassment, misogyny, hate speech violate women, LGTBQI and other marginalised groups rights to privacy, work, public participation, freedom from violence and freedom of expression and opinion.

As seen in the previous section, WHRD, women net activists and their allies are using digital technologies to engage in debates, to document, raise visibility, network, provide emergency response and direct services to people facing violence. Through the organisation of the GTI and other related training activities, we have helped WHRD and activists to understand how their issues are being affected by the ways in which offline discrimination, control and abuse play-out in online environments and to find strategies for handling the barriers posed to their free expression online. We have supported them to design their outreach considering the tension between exposure and participation by carefully assessing the potential associated risks as well as the available mitigation strategies and tools. We have enabled them to better navigate the challenges of expression and security online.

We have also collaborated with those in our sector working on different aspects of this challenge strengthening networks and partnerships for women's rights activists in key global regions and complementing the work of policy and research work of partners, such as the APC Women's Rights Programme. We have seen that we can develop partnerships, build skills in the community, and on the ground level enable women to better protect their privacy and the privacy of their communities, in order to keep using online spaces for expression and association and to defend their rights.

Through this project, Tactical Tech has contributed to the building of the skills

of a diverse network of women from different communities and regions, who as a result of the activities can conduct trainings and awareness raising events, in turn reaching a broader scope of key players. We have been working with this community to develop and run privacy advocacy and digital security trainings with a gender perspective. Besides, we have developed - in interaction with them - a set of self-learning resources that have been tested and distributed through the different workshops organised on the ground. The involvement of trainees in co-designing and producing new toolkits and documentation such as the Gendersec wiki and the manual have enable more targeted contents that fit community driven needs and interests.

The solutions proposed in this project have therefore begun to solve the above defined problems as follows:

- Develop capacity within the women's rights and empowerment sector by training women trainers and women net activists who have become go-to people within their own communities within different regions.
- Building a strong international network of support among women trainers who can work across and though the women's rights sector.
- Closing the information and awareness gap about the challenges to freedom of expression and association for women online, creating a move from analysing and understanding the challenges to providing practical advice and support to women net activists and stimulating discussion about strategies for navigating these challenges.
- Support women journalists, activists and others who have an influential social media presence who can act as engaged advocates for women's security online by being more confident and engaged themselves in implementing digital security and privacy-protecting behaviors.
- Implement trainings that not only transfer skills but also allow the community to better understand the issues and find solutions.
- Create learning resources and adapt curriculum which can be shared through creative commons licensing and at the same time allow for further documentation of the needs in the sector.
- Including gender by placing privacy and digital security within a broader

holistic approach which moves away from militaristic and patriarchal definitions.