CYBERWOMEN

INSTITUTE FOR
WAR & PEACE REPORTING
IWPR

# Holistic digital security training curriculum for women human rights defenders

# Introduction to Cyberwomen

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

# Contents

**1 Introduction to Cyberwomen** **5**

Using the Cyberwomen Curriculum . . . . . . . . . . . . . . . . 6

# Chapter 1

# Introduction to Cyberwomen

Within the last few years, various efforts have been undertaken to create improved resources, methodologies and practices for digital security trainings; however, very few of the resulting outputs have incorporated a strongly developed gender perspective. More recently, thanks to efforts within women's and feminist movements worldwide, a body of gender focused digital security content has begun to emerge – however, there remains a lack of coordination within the digital security community to grow this collection of resources in a strategic, responsive manner.

To that end, the Institute for War and Peace Reporting (IWPR) built the Cyberwomen curriculum with the intention of reflecting the rich technique and practice developed by women human rights defenders (WHRDs) leading digital security training efforts in the Latin America and Caribbean (LAC) region. Based on the experience of working with these women, we have created original training content with the aim of presenting a collaboratively-developed approach for training WHRDs on digital security from a holistic, gender-based perspective.

To avoid duplication of efforts, where we identified existing training materials already responsive to the needs of WHRDs – for example, those found within the LevelUp curriculum, or developed by organizations like Tactical Technology Collective (TTC) and Association for Progressive Communications (APC) - such content was incorporated directly into the curriculum and cited accordingly. However, the core value-add of this resource lies in originally-produced modules and recommendations designed to offer learning experiences specifically tailored to the context of WHRDs working in high-risk environments.

## Using the Cyberwomen Curriculum

This curriculum was designed with two specific user-profiles in mind: women trainers seeking to deliver gender-focused digital security trainings to women's groups, and members of these women's groups who, after receiving such training, now seek to pass that digital security knowledge onward to their own networks of colleagues and activists. In truth, not all sessions may be relevant to all audiences, and we encourage you to identify which sessions are most valuable for your specific audience and focus exclusively on those.

Cyberwomen includes interactive games, as well as audio-visual and graphic materials, as instructional aids for trainers; furthermore, its modules can be used either as stand-alone sessions or as components of a full training workshop. This modular structure allows trainers to select specific session content to match the needs of training participants; alternatively, trainers may also choose to follow suggested sequences of modules. From start to finish, to cover the entire curriculum would require approximately ten full days; for those trainers who wish to provide such a training, we strongly recommend separating delivery out into a series of workshops spaced over a period of at least six months. This approach will allow participating women the time required to effectively integrate new techniques and tools into their personal digital security practice, before moving on to acquire new skills.

Furthermore, as part of its focus on holistic security, the curriculum incorporates specific content on feminist self-care and recognizing gender-based violence, whether symbolic or online. The objective of these sessions is to reinforce participants' sense of agency and control over their safety and identities – therefore, it is important that they be integrated throughout trainings as spaces for individual and collective action and reflection, rather than covered as a standalone module by themselves.

Finally, there are many exercises included in this curriculum - some are trust-building exercises, which should be done at the beginning of the first training day; others are basic icebreaker exercises, which can be done at the beginning of any training day. Finally, there are several exercises designed to reinforce specific training content which should only be done in their listed order. The curriculum also includes resources for follow-up sessions to be delivered over the suggested period of six months.

### A Feminist Approach to Curriculum Development

As mentioned previously, this curriculum integrates a holistic vision of security for WHRDs, including the "Triad" of digital security, physical security and self-care; however, the core of the training is focused on digital security. To integrate a more gender-sensitive, feminist approach, this curriculum was produced with the following core values and principles in mind - we strongly encourage trainers to take these into account while planning workshops using this curriculum:

### Women Participants and Women Trainers

First and foremost, Cyberwomen content is designed to support an ambiance of woman-to-woman confidence and trust in a training setting. Participants in digital security trainings frequently come from places – both physical and emotional – of high stress or anxiety; women human rights defenders are also frequently the targets of harassment and violence both online and offline. It is paramount that women participants perceive a training as a safe space, where they can feel at ease sharing their fears, doubts and emotions, and can actively participate and engage with others; therefore, this curriculum is intended for women trainers working with women participants. However, we also encourage male trainers to review this curriculum and its foundational principles to better adapt their own training practice to working with mixed groups in a workshop setting.

**Female and Feminist Models**

This curriculum was created with a focus on sharing real-life instances of digital attacks - as experienced by women human rights defenders, activists and journalists - using empowering testimonies. Recognizing that not every woman at a given workshop will define herself as a feminist, the curriculum's approach to the training process focuses on raising awareness about online violence against WHRDs, first by highlighting differences between attacks on male and female activists, and then by providing examples of online gender-based violence (e.g. on social media platforms) as a means towards helping women identify the violence they may already be facing in these spaces. As part of this methodology, we presented case studies that were close to the women's everyday life, making it easier for participants to relate to different situations and thus understand the relevance to their own context. We found that using this approach empowered participating women to more consistently practice new skills and subsequently provide digital security advice to others.

**My Body, My Devices, My Decision!**

The central ideas, information and practices shared in this curriculum are grounded in promoting digital autonomy. Central to the design of this curriculum is an emphasis on "strategic thinking about digital security" - sharing digital security concepts with participants, rather than just training on a list of tools. A great deal of time is dedicated to introducing participants to digital security concepts such as encryption, anonymity, privacy and open-source software before training on related tools. By empowering women to develop a personalized understanding of these concepts, they come away equipped with the information they need to make their own decisions about which tools are best for them.

### Analysis of Gender-Based Risk and Social Media

By using examples from YouTube videos, messages on various social media platforms, and outputs emerging from other training sessions, this curriculum aims to hold a safer space for discussion and reflection on technology-based violence that specifically targets women. Specifically, much of this comes together in the Online Violence Against Women module; likewise, the Gender-Based Risk Model exercise found in the module Determining the Best Solution is focused on sharing experiences and identifying vulnerabilities participants face not only as women but as human rights defenders (in this case, in the LAC region).

### Feminist Self-Care & Digital Self-Defense

As part of a holistic approach to security, this curriculum considers emotional well-being and self-care as a vital element of security for WHRDs; likewise, as part of a focus on digital autonomy, there are specific sessions —the session Gender-Based Risk Model again serving as an example— which are intended to help participants prepare for and react to digital attacks. This curriculum is an effort to provide information for participants to identify and explore several strategies for their digital self-defense; these include, but are not limited to, separating the personal from the public, creating online identities, 'doxxing the troll', encrypting their communications, and documenting digital incidents. By equipping participants with a better understanding of their online environment —across both the platforms they use and the risks associated with each— we can empower them to develop strong digital security habits that can in turn become part of a holistic practice of self-care.