Digital safety workshop

Digital Defenders Partnership

The Digital Defenders Partnership offers support to human rights defenders under digital threat, and works to strengthen local rapid response networks.

https://www.digitaldefenders.org/
Shared Agreements

• Confidentiality. We commit ourselves not to comment outside the group what has been shared on a personal level during the sessions. Accordingly, we will not record the workshop in order to protect the confidentiality of the information shared during the workshop.

• We will not admit discriminatory attitudes or comments: sexist, homophobic, racist, transphobic, ableist, fat-phobic, specist etc.

• We are open to learn from each other. There are no stupid questions. This sessions might open a lot of questions and doubts, we will list these in case they can not all be answered during the sessions.

• We will self regulate the amount of space we take. We try to speak briefly and concretely. So that everyone can participate, we try not to take up too much time and not to repeat ideas. The facilitators will encourage those who have spoken less to participate.

• We practice active listening. We will listen to the others without judging, interrupting, advising or saying what the others should do, even when we do it with good intentions.

• We will accept that there will be objections and different points of view. We will pay attention to how this diversity enriches us.
Risks and vulnerabilities faced by migrants + refugees and the CSO supporting them

- Information communication technology (ICT) encompasses the tools and platforms we use for our communication, information, documentation, relation, identity making needs. ICT are also crucial to our production of narratives and imaginaries.

- These can be analogue or digital formats, including radio, television broadcasts, mobile phones and the internet. ICT has become a fundamental part of our daily activities, merging digital and physical spaces.

- Almost everybody uses or is impacted by ICT nowadays.

- The needs, uses, risks and threats faced by migrants (documented/undocumented) and refugees (transitioning) and the CSO supporting them share common points and differences too.
Migration Management Technologies

- These technologies are funded by big companies and the military complex.

- They include Big Data predictions about population movements in the Mediterranean, to Canada’s use of automated decision-making in immigration, to Artificial Intelligence (AI) lie detectors at European borders.

- AI, facial and posture recognition, Wifi tracing, thermal imaginary all have bias and a strong impact on marginalized and discriminated communities (BPOC, women, migrants, refugees)

- Automating Migration Decisions also raises issues of informed consent, particularly in the increasing reliance on biometric data.

- How do you challenge these automated decisions? Where does the responsibility lay on?
Migration Management Technologies

These technological experiments often fail to account for profound human rights ramifications and real impacts on human lives.

Currently, new technologies in migration are largely unregulated. More global oversight and accountability mechanisms are needed to safeguard fundamental rights such as freedom from discrimination, privacy rights, and procedural justice safeguards such as the right to a fair decision-maker and the rights of appeal.
Migration Management Technologies

Varoon Mathur, AI Now's Tech Fellow, 2018 AI scandals review
'Social media monitoring' (sometimes also known as ‘SOCMINT’) is the analysis of the content and metadata of people’s social media posts, for example, to identify the political views, and relationships that you have with others online. It may include snooping on content posted to public and even private groups and pages. And it may involve ‘scraping’ of data, which in effect enables someone to collect and analyze a huge amount of data about you, and then easily build profiles and predictions about you.

Privacy international, A guide for migrants and asylum rights organisations about privacy settings
Digital litter and Social Media Infotoxication

- Access to a smartphone and the digital infrastructure of wifi, simcards, charging docks, and electricity has been described as a literal lifeline.

- High exposition to digital litter: «Poor-quality information spread online or through digital tools, apps, and social media is undermining refugee and migrant decision-making and placing them in harm’s way. Dozens of clearinghouses, online maps, and platforms purporting to consolidate educational and other opportunities for refugees are now full of broken hyperlinks or touting things that no longer exist».

- Infotoxication and hate speech: inaccurate information, including false rumors and conspiracy theories, but also fraud with false employment offers can make them more vulnerable to exploitation or physical harm during transit
Today, subtle but pervasive forms of online transnational repression are increasingly common. Activists living outside their homeland are now more likely to encounter digital surveillance, threats, and smear campaigns designed to stifle their opposition and induce self-censorship.

The tools most often used in the cases of Egypt, Syria, and Iran include online monitoring and surveillance, account and device hacking, aggressive disinformation campaigns, and online publication hacking. The principal aim of these practices is to spread insecurity and mistrust in transnational networks, silence dissidents living in exile, and undermine cross-border relationships between exiled activists and their homeland communities.
Gender Based Violences
Anonymity and digital privacy are a critical part of human rights, but they are also connected to cyber crime, such as fraud, identity theft, cyber stalking, bullying, phishing and trolling. Survivors of GBV rely on anonymity and privacy to access life-saving information, while abusers use these rights as an opportunity to commit violence freely.

Source: Take back the tech
Q/A and comments about the collective mapping of risks and vulnerabilities
Holistic Security

⚠️ Physical Security
Threats to our physical integrity. Threats to our homes, buildings, vehicles.

⚠️ Psycho-social Security
Threats to our psychological wellbeing.

⚠️ Digital Security
Threats to our information, communication and equipment.

Holistic security analysis, strategies and tactics.

Holistic security Manual
https://holistic-security.tacticaltech.org/
Security perception and needs are...

- Subjective, each person has it own perception
- Contextual, the security needs are based on a context, they depend of what you are doing, your social relations, your social and political context, your networks for support
- Perception and needs change over time and need to be revisited frequently
- Security needs require to do security assessment/diagnosis, threat analysis
- Individual needs for security are different of needs for security of an organization, a collective, a loose network

Holistic security Manual
https://holistic-security.tacticaltech.org/
Organizational security

- Creating safe spaces that are selectively inclusive and empowers people.
- It consists of process (implementation, support and development) and resources (people and technology).
- Organizational control of data and how it is used (and by whom) - without any loss of control.
- Facilitating their work with communities through strong reputational trust.
- Composed of different aspects of risk management including physical, digital, psycho-social, legal, health.
- Organizational ability to conduct their work safely, sustainably, and responsibly.
- A group with common operational and substantive aims, with shared and agreed practices towards protection from threat, integrity of systems, and the safety and wellbeing of individuals.

Orgsec community, https://orgsec.community
### Personal data

<table>
<thead>
<tr>
<th>Personal Identifiable Information (PII)</th>
<th>Personal Sensible Information (PSI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Ethnic origin</td>
</tr>
<tr>
<td>Legal name</td>
<td>Religious beliefs</td>
</tr>
<tr>
<td>House address</td>
<td>Political beliefs</td>
</tr>
<tr>
<td>Phone</td>
<td>Sexual orientation</td>
</tr>
<tr>
<td>IP address</td>
<td>Gender identity</td>
</tr>
<tr>
<td>MAC address</td>
<td>Medical history</td>
</tr>
<tr>
<td>Car registration</td>
<td>Jail or legal history</td>
</tr>
<tr>
<td>Social security number</td>
<td>Travel records</td>
</tr>
<tr>
<td>Pictures</td>
<td>Social networks</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Activist or HRD trajectory</td>
</tr>
<tr>
<td>Iris</td>
<td></td>
</tr>
<tr>
<td>ADN</td>
<td></td>
</tr>
</tbody>
</table>
Security assessment and threat analysis

What is the best methodology? It depends, individual or collective analysis? Formal organization, community, informal collective or a loose network?

1) Places you within a group that may have certain types of vulnerabilities.
2) It invites you to identify adversaries (and groups them by type of adversary).
3) It gives you a risk model
   Risk = (threats x vulnerabilities) / resilience capabilities
4) Gives you a vocabulary for threats
5) Generates a feasibility analysis impact = level of threat
6) Identifies what you are looking to protect

Modelador de riesgos
Q/A and Comments
Identifiable Personal Information (IPI) + Sensible Personal Information

Localisation
Geographic + IP

Social networks/Contacts

Contents
Communication
Fortification

- Barriers, restrict, monitoring, detection, quarantine, migrate

Obfuscation

- Lying / False positives
- Making noises / Rumours
- Hiding (in the multitude)
- Camouflage / Make-up
- Change routines

Compartimentalisation

- Separate / Split
- Dissociate / Don't link
- Map / Classify

Cleaning / Disposal / Destruction / Destruction

- Organize / Range
- Ignore / Block / Resist
- Recycling / Equipping new uses

Reduction

- Less = Better!
- Generate a lack of data and information

More = Better:

- Inflation of Data / Information to devalue its value

My devices, My rules!
<table>
<thead>
<tr>
<th>Identities Management</th>
<th>Risks</th>
<th>Reputation</th>
<th>Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Name</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Anonymity</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Pseudonym</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Collective identity</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
Evaluation