www.donestech.net

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

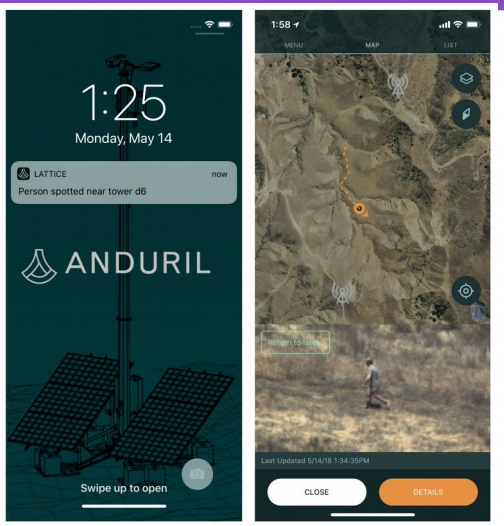
- Information communication technology (ICT) encompasses the tools and platforms we use for our communication, information, documentation, relation, identity making needs. ICT are alo crucial to oir production of narratives and imaginaries.

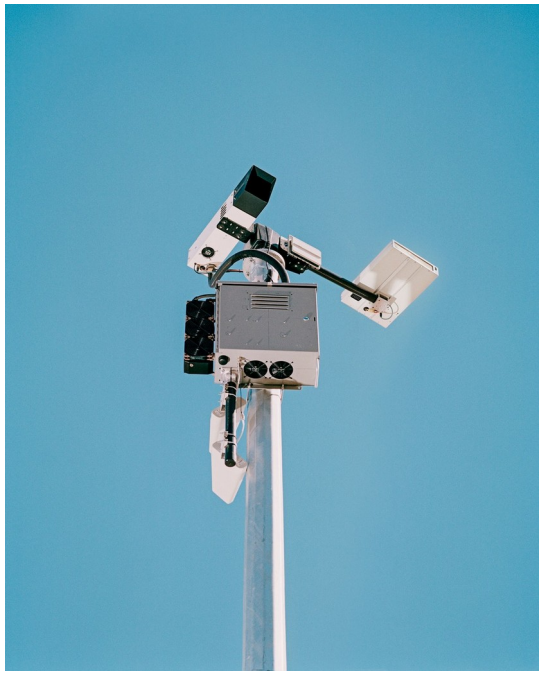
- These can be analogue or digital formats, including radio, television broadcasts, mobile phones and the internet. ICT has become a fundamental part of our daily activities, merging digital and physical spaces.

- 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

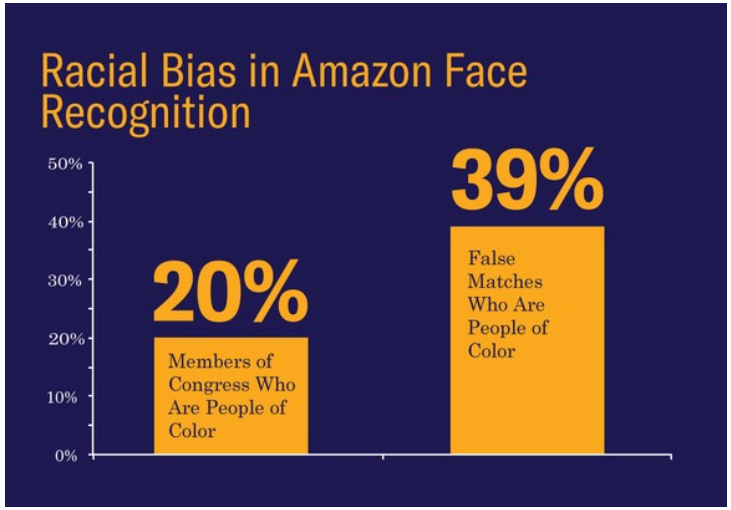




- These technologies are funded by big companies and the militaro complex.
- They include Big Data predictions about population movements in the Mediterranean, to Canada's use of automated decision-making in immigration, to Artificial Intelligence (AI) lie detectors at European borders.
- AI, facial and posture recognition, Wifi tracing, thermal imaginery all have bias and a strong impact on marginalised 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 responsability lay on?

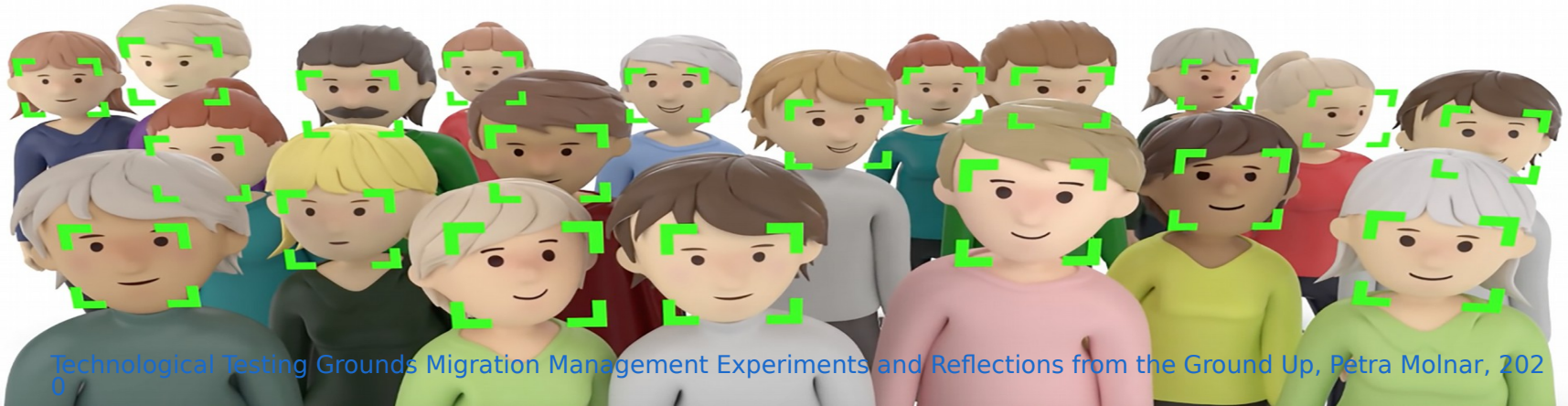
Technological Testing Grounds Migration Management Experiments and Reflections from the Ground Up, Petra Molnar, 2020

Migration Management Technologies



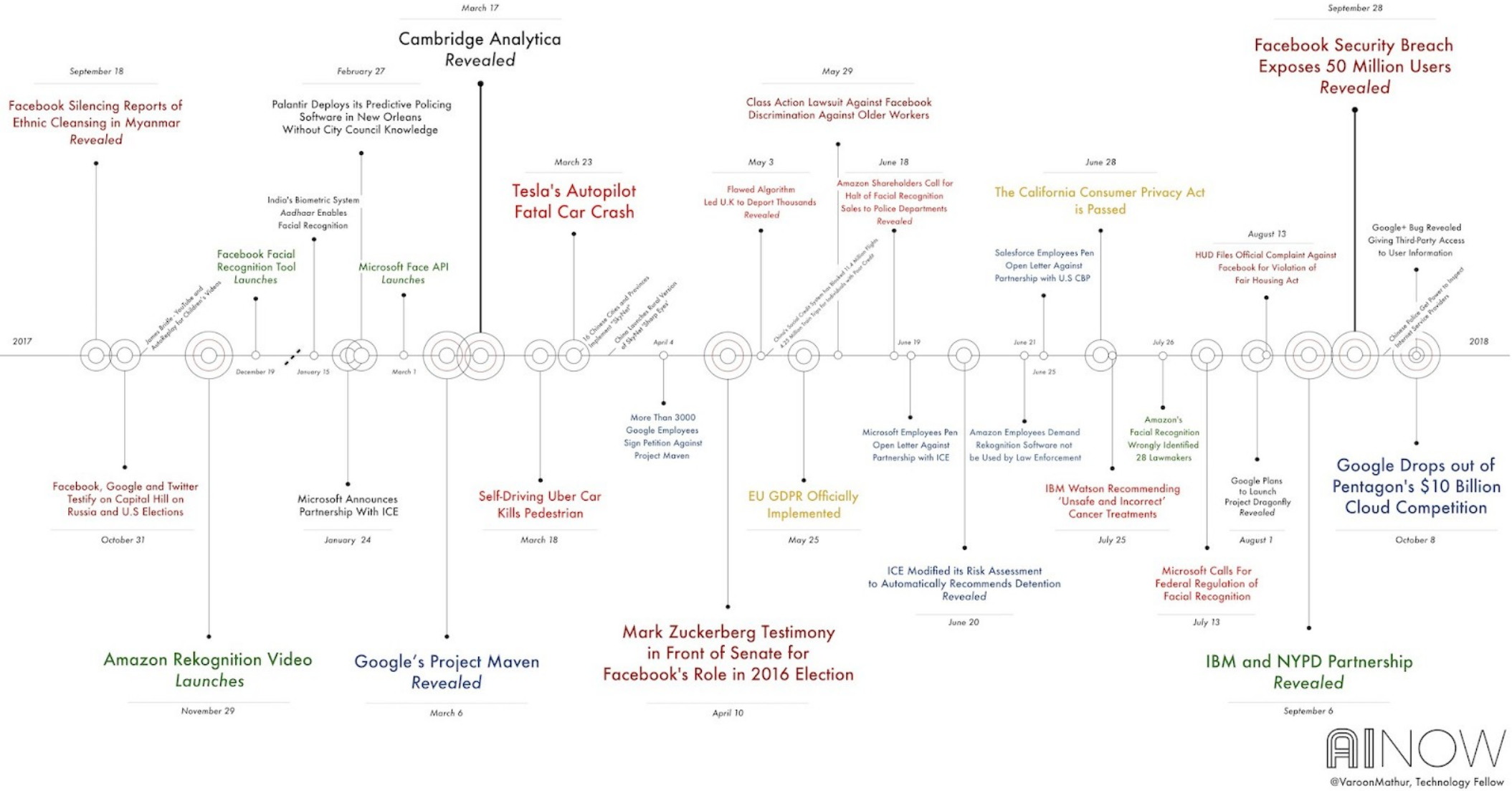
These technological experiments often fail to account for profound human rights ramifications and real impacts on human lives.

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



Technological Testing Grounds Migration Management Experiments and Reflections from the Ground Up, Petra Molnar, 2020

Migration Managament Technologies



Varoon Mathur, AI Now's Tech Fellow, 2018 AI scandals review

Social Media Monitoring

'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 analyse 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 org anisations 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 liter: «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 employement offers can make them more vulnerable to exploitation or physical harm during transit

Digital Litter: The Downside of Using Technology to Help Refugees

Moverse seguras y seguros, 2021. TCM.

Transnational repression using ICTs

SILENCING ACROSS BORDERSTRANS NATIONAL REPRESSION ANDDIGITAL THREATS AGAINST EXILEDACTIVISTS FROM EGYPT, SYRIA, AND IRAN

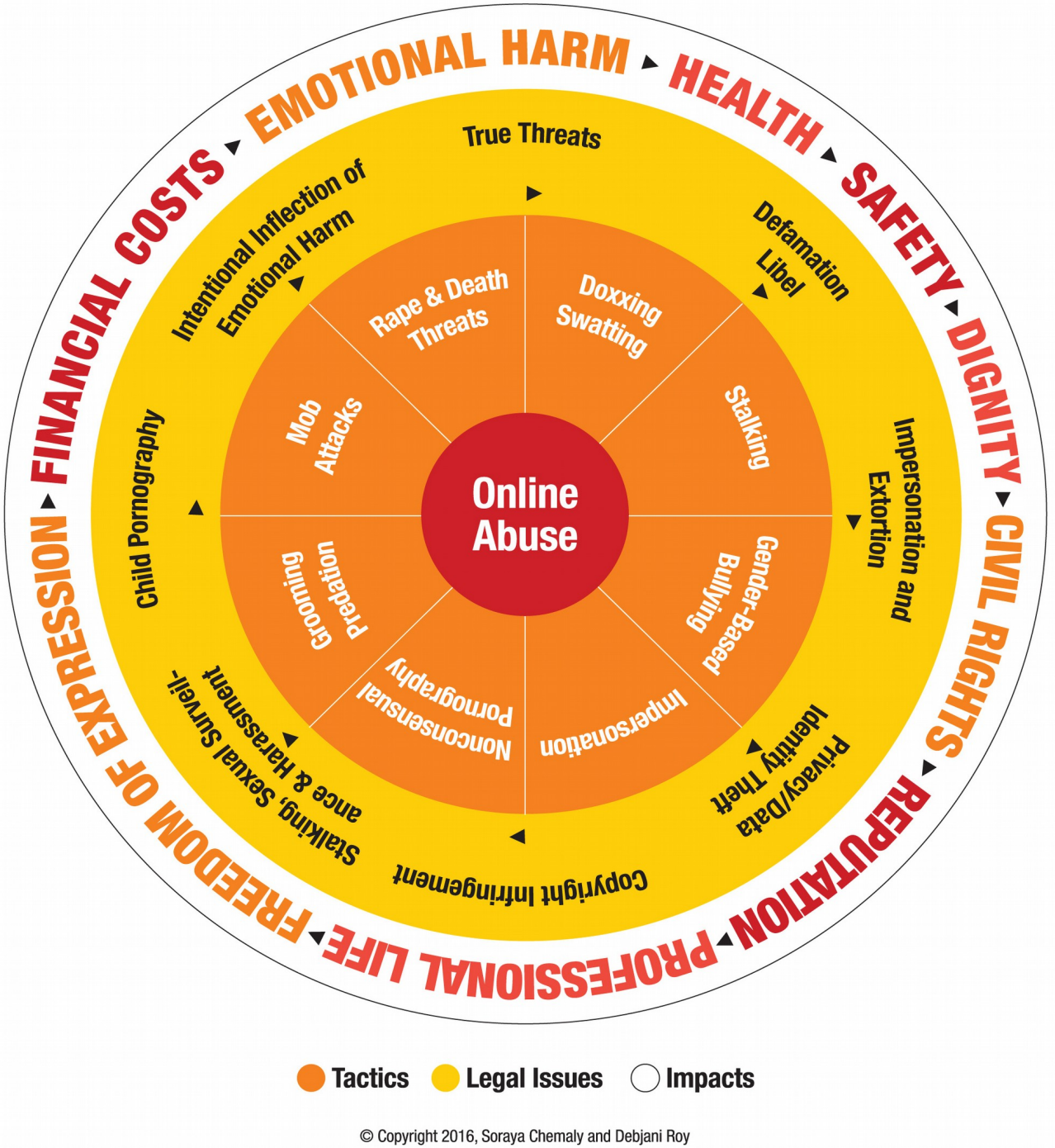
,

Marcus Michaelsen, 2020

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

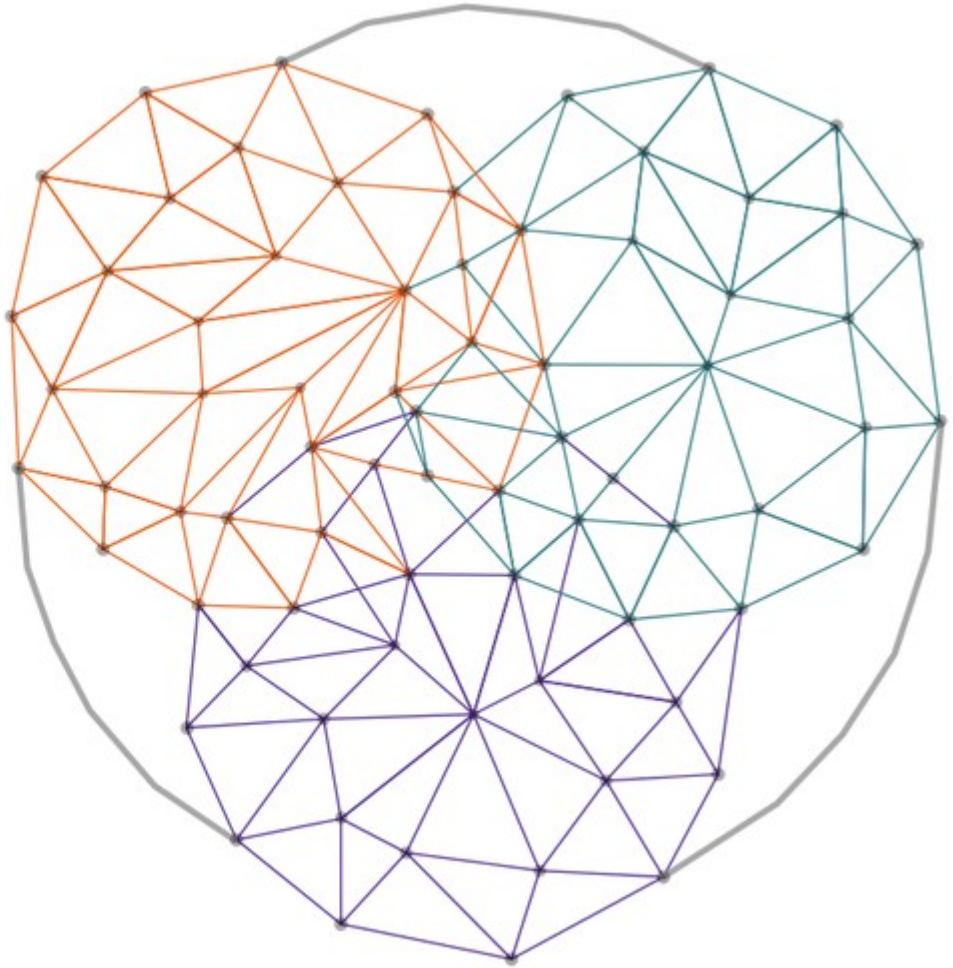
Holistic Security

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

△ **Psycho-social Security**
Threats to our psychological wellbeing.

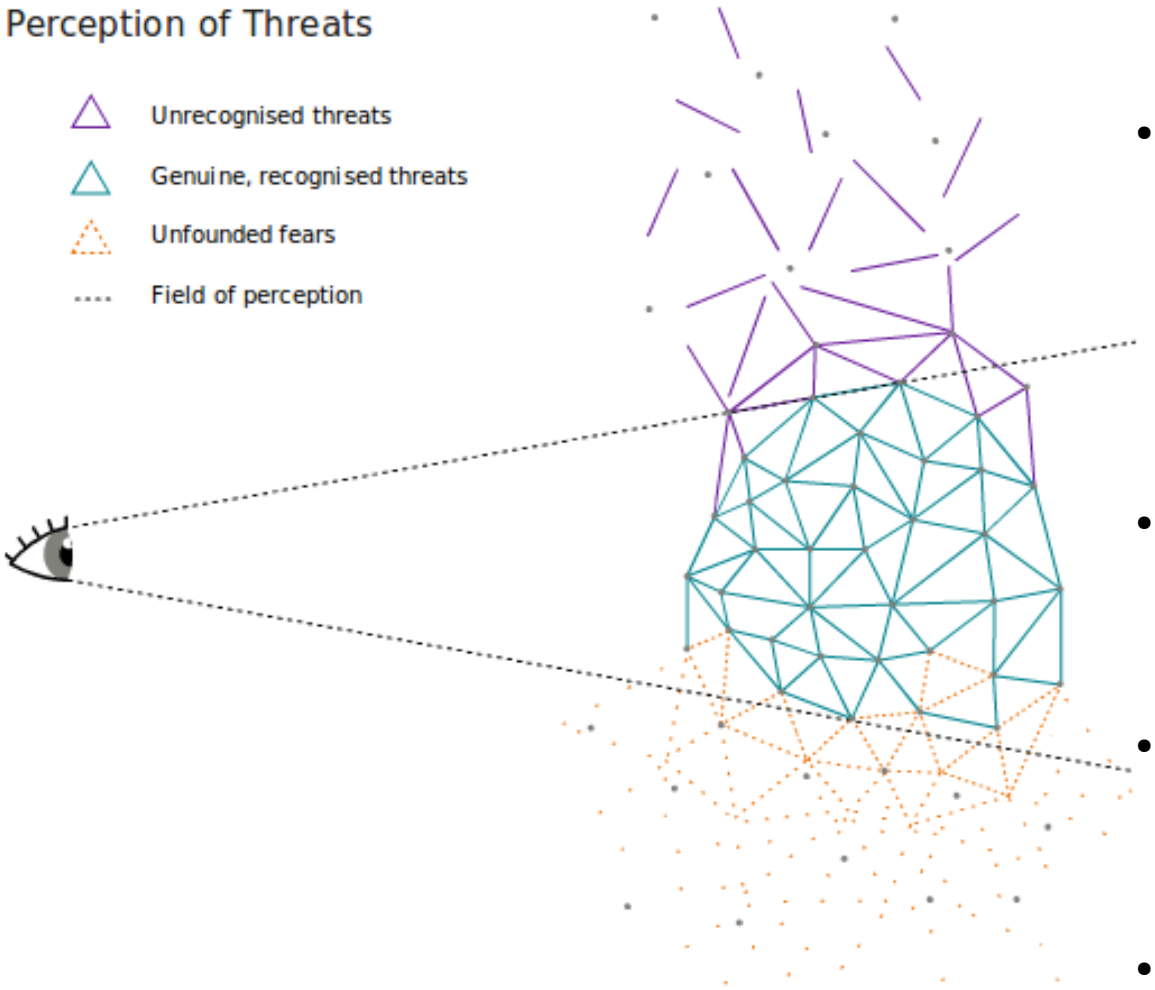
△ **Digital Security**
Threats to our information, comunication and equipment.

— Holistic security analysis, strategies and tactics.



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

Security perception and needs are...



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

- 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 assesment/diagnosis, threat analysis
- Individual needs for security are different of needs for security of an organisation, a collective, a loose network

Organisational 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, psychosocial, 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

Digital Defenders Model of accompaniment of CSO:
https://manuals.digitaldefenders.org/

DDP ‘Holistic’ Security Accompaniment model

Between 6 and 18 months of accompaniment + training of 2 security focal points members of the organisation

Infrastructural support

Legal support

Psycho-Social support

Physical support

Addressing Gender & Diversity Inequalities, Social economic imbalances, Political repression; with a Do-No-Harm approach, and from a conflict-resolution point of view

Personal data

Personal Identifiable Information (PII)	Personal Sensible Information (PSI)
ID Legal name House adress Phone IP adress MAC adress Car registration Social security number Pictures Fingerprint Iris ADN	Ethnic origin Religious beliefs Political beliejs Sexual orientation Gender identity Medical history Jail or legal history Travel records Social networks Activist or HRD trajectory

Security assessment and threat analysis

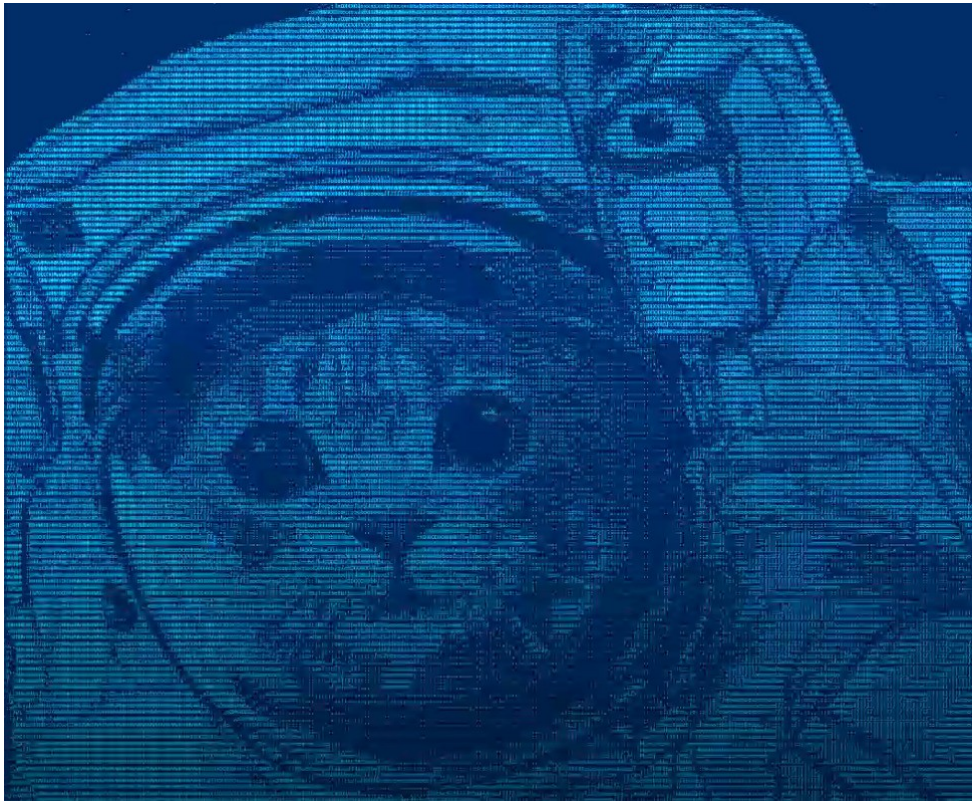
What is the best methodology? It depends, individual or collective analysis? Formal organisation, community, informal collective or a loose network?

- What do I want to protect and is worth protecting?
- Who do I want to protect it from?
- How likely is it that I will need to protect it?
- How bad are the consequences if I fail?
- How much trouble am I willing to go through to prevent these consequences?

Your security plan by Surveillance self defen se

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

My devices, My rules!

Reduction

Cleaning/Disposal/Destruction/ Destruction
Organize/Range
Ignore/Block/Resist
Recycling/Equipping new uses

Less = Better!
Generate a lack of data and information

Obfuscation

More = Better:
Inflation of Data/information
to devalue its value

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

Compartimentalisation

Mix and combine:
Diversity of profiles,
each one with its own value

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

Identities Management

	Risks	Reputation	Effort	
Real Name	+	+	-	
Anonymity	-	-	+	
Pseudonymie	-	+	+	
Collective identity	-	+	+	

Evaluation