Image not found or type unknown

Risk assessment in movement organising [foundational material]

Overview

When thinking about risk assessment at the level of movement organising, it means expanding the scope of consideration to also include shared spaces, processes, resources or activities that are helmed collectively – formally or informally.

Movements are larger than an organisation, and made up of relationships of shared political commitment and action between different actors. Movement actors can be comprised of individuals, organisations, collectives, community members or groups, and bring different knowledge, skills, contexts and priorities into a movement. How movement actors organise themselves, figure out roles and areas of responsibilities and come to agreements are important dimensions of movement organising, where risk assessment can also play a part in surfacing potential points of stress.

Risk assessment from a movement perspective

It's often easier to identify movements from hindsight, as they grow organically through time and in response to concerns of specific contexts and moments. Sometimes, we think of movements as protests, since that is often the site where many movements are visible and grow. But not all

movements end (or begin) in protest. For example, many LGBTIQ++ movements in places where visibility carries a high cost organise and take action in less visible ways, such as creating closed community spaces online, where individuals can convene, converse, provide support and strategise for different kinds of interventions.

A movement is made up of many different moments or stages, such as community outreach, building evidence, deepening understanding, consensus building, taking action, holding space for collective care, distribution of resources and so on.

Each of these moments or stages can be specific times in which collective risk assessment can be undertaken by those who are holding space or process. It might be useful to think about movement security as having the conditions in which the many stages or components of movement work can take place and thrive.

Layers of risk

One way to begin the process of risk assessment from the perspective of movements is to unpack the different layers that need consideration. There are three components that interplay with each other.

1. Relationships and protocols
2. Spaces and infrastructure
3. Data and information

The next sections describe what each layer is about, and some of the components within them, including questions for discussion that can help to unpack, analyse and understand the risks, towards coming up with a plan.

1. Relationships/protocols

At the heart of strong movements are strong relationships which are built on the basis of trust. This is particularly important as movements are less about form than about the strength and tenacity of their relationships at different levels.

Risk assessment can take place at the level of the individual, organisation or informal groups. When approached from a movement building perspective, it means paying attention to the relationships between those levels.

For example, if an individual is undergoing a lot of stress because they are working from pay check to pay check, this can affect their ability to participate fully, which in turn can impact on the organising work as a whole. Or if an organisation is under attack by the government, its affiliation to other organisations or individuals in the movement can also render them open for similar attacks. Or if there is abuse between members of a collective, this can weaken the movement as a whole from both external as well as internal stresses.

In other words, risk from a movement perspective is something that is taken on collectively, and is affected by the practices and well-being of the different nodes/actors who are part of movement organising.

To manage risks at the level of relationships, the following three areas can be looked at:

a) Collective care

Collective care is both an individual responsibility and a matter of collective accountability to each other. This means that assessing and planning for risks needs to take into consideration different individuals' state of well-being, as well as in relation to each other in terms of shared spaces, platforms, resources and processes.

- What are some of the risks to well-being currently faced by different actors in the group?
- What may some of the impacts be?
- What is the technology layer to this question around care and well-being? For example, are there protocols around switching off from social media, limits to online meetings, or enacting bystander solidarity activism when a member is attacked?
- How can some collective practices be developed to mitigate or address some of the risks or impacts? Are there resources or skills that can be pooled together or shared? For example, can different organisations or individuals pool funds together to subscribe to a more secure communication channel or hosting platform that allows for greater control over data?

b) Inclusion and representation

This is in terms of processes and criteria for including people into different layers of organising spaces. Sometimes this is only considered when a security breach has happened, such as information about an event being leaked to hostile parties because everything happens in one WhatsApp or Facebook group. Thinking about inclusion mechanisms can help in being more purposeful in developing different security levels of information sharing and communication channels. Thinking about representation in movement activities can help to also surface particular risks to individuals or groups of people, and how to mitigate, distribute or prepare for this risk.

- What are the protocols around bringing in new people, or when people leave? For example, mailing lists or other kinds of discussion and work spaces.
- Are there specific risks around having many or singular faces to visible moments of the movement? How can this be planned for? For example, when a call for participation is being published, is there a plan for which accounts this should come from (personal accounts, single-use accounts set up for the specific activity, organisational accounts, etc.), and timing so that it cannot be traced back to one initial source?
- What are some of the risks associated with solidarity actions with allies in a particular instance, and how can this be planned for? For example, highlighting consent around documenting and posting pictures in social media, especially of targeted identities, or distributing risk by having many people.
- What are the different internet connectivity and technical capacity contexts of those within the movement – and how does that affect their ability to securely participate in the movement?

c) Managing conflict

This is often an area that is least addressed within movements, as we assume shared politics, values and interest. However, it’s important to allow for these to be surfaced, discussed and planned for, as they can serve to support the overall justice mission of the movement, as well as ensure that internal vulnerabilities or power differences are addressed.

A plan doesn’t have to be complex, but it can begin with a frank and carefully held discussion, surfacing shared values and coming to agreements, and then making a plan around this including who should be involved, what measures can be taken, and how shared values can be collectively enacted.

- What are some of the potential conflicts that could present as risks to a movement? In particular, conflict between members – what might the impact be? For example, loss of trust, community members taking sides, loss of control over movement resources such as passwords, access to sites, etc.
- How can a response plan be developed for different kinds of conflict? For example, sexual harassment within the movement, intimate partner violence between members of the movement, romantic or sexual relationships between members of the movement that ended badly, decision making around shared resources or funding, disagreements around core values or strategies, etc. Some of these are longer-term, sustained mechanisms, while others may be contingent upon specific activities.

2. Spaces/infrastructure

The digital layer is an increasingly critical component for organising and movement building in current times. Because movements are not located within an institutional space, digital infrastructure and platforms become an important shared space for coming together, coordinating and planning activities, documenting decisions/transparency, as well as the living archive of collective history, etc. It's a critical part of the ecosystem of movements today.

Often, digital infrastructure of movements is a combination of different platforms, tools and accounts that are employed or emerge across time in evolution with the movement as it grows. Unlike within an organisation, there may be several people taking care of different kinds of spaces for different purposes, which may also serve different communities. Some of these could be personal accounts, some could be temporary accounts set up for an activity or event, and some can be subscriptions and spaces created specifically for a coming together of different information, content and community streams. Taking a moment to understand this as an ecosystem – interconnecting components of a shared movement infrastructure – and to assess potential risks can help to surface collective responsibility, care and stewardship over these spaces, as well as to develop safety plans around potential compromises.

The following areas can be discussed when thinking about risk assessment on spaces and infrastructure, with some questions that can be considered:

a) Platform/tool/hosting decisions

Movement and organising work relies heavily on information sharing and effective communication. As such, thinking through risks related to which platform or tool to use for organising, and where they will be stored, can have a large implication on the safety and security of the people, groups and work of the movement. In assessing risks related to vulnerability to breaches and attacks, it may be useful to consider if there are feminist/activist-developed or hosted solutions for that specific need, as they generally pay greater attention to issues of privacy and security.

It’s also important to consider accessibility, usability, ease and likelihood of effective adoption by larger movement members. It’s not always useful to choose the most technically secure solution, when it requires a lot of investment in time and energy to learn how to use it, which may not always be possible or preferable.

- What are the current platforms, tools and spaces being used, for what purpose, and who has access to them?
- What are the potential risks associated with particular platforms/tools/hosting for the need at hand? What are the impacts of these risks?
- What are the literacy, skills and capacity needed for adoption? How can these literacy, skills and capacity be shared and built with wider pools of people within the movement to not create an internal technology-based power hierarchy?
- Is this platform/tool accessible to most people who need to use it? Will barriers to ease of use end up creating more insecure practices instead? How can this be addressed?
- Can risks be distributed by also distributing platform/tool use for specific purposes?

b) Ownership and resourcing

Ownership and management of shared digital infrastructure is both responsibility as well as power and potential gatekeeping. The more a movement is able to surface this as a political conversation around shared values and understanding on governance, economy and community building, the more sustainable some of the shared technology practices can be.

- How will use of specific infrastructure, platforms or tools be resourced? How are they currently resourced? What are the internal shared movement economics of distributing costs when it comes to use of and commitment to particular technology(ies)?
- What are the risks of use of “free” platforms when it comes to control over data and functions, and the risks of paid services when it comes to ability to commit to costs for a sustained period of time? How can these be planned for?

- How can this also be reflected in the politics of the movement? For example, developing protocols around common ownership, management and resourcing. Can ad hoc, informal and light cooperative economic arrangements be made? How can these be sustainable and transparent?

c) Administration and protocols

In the context of movement organising, thinking about infrastructure as shared space means that having clarity around how these spaces are managed and by whom can help to surface not only collective care, but also potential risks related to access to, care of and potential loss of information and community space.

- Who has control over access to specific spaces? How much of this is about who owns the space (personal accounts) or settings, and how much is it about literacy, device or connectivity preconditions for access?
- What are the risks involved in compromises to specific spaces? Where might these compromises come from (think of both internal and external threats), and what might the impacts be? How can this be planned for?
- How are spaces managed? And what are the protocols for e.g. how many people have administrative access, their location (individual, organisation, network), how often this is changed, conditions for change, changing passwords, etc.?
- Are there protocols around deleting spaces or data, and archiving? Or are there existing practices that can be discussed and translated into protocols?
- How, where and when do discussions about risk assessment on shared digital infrastructure happen?
- Who will respond if there are incidents within spaces/infrastructure that affect the safety and security of the movement?
- What changes in the spaces that the movement uses (e.g. new security policies in platforms, the removal of security features, etc.) and within the context of the movement (e.g. changes in country situation, changes in government, new laws that affect the ability of the movement to continue its work, etc.) will trigger a larger discussion within the movement about its spaces/infrastructure? Who will monitor these changes?

image-1605451259399.png
Image not found or type unknown

3. Data/information

Data and information are being produced and generated all the time while organising. This can be in the form of formal or informal, deliberate or shadow forms of data. Another way to understand risks in increments is to look at the data practice of a specific activity or strategy of a movement. Think about this from either a specific working group within a movement that is responsible for carrying out specific tasks or strategies, or from the perspective of an activity. This can also be used at the level of an organisation, as every organisation deals with data, and each unit within an organisation does as well.

Here, there are some security and safety considerations for each phase of the data life cycle. There is an activity called "Data life cycle to as a way to understand risk" that operationalises this section.

a) Creation/gathering/collection of data

- What kind of data is being gathered?
- Who creates/gathers/collects data?
- Will it put people at risk? Who will be put at risk if this data is released?
- How public/private/confidential is the data gathering process?
- What tools are you using to ensure the safety of the data gathering process?

b) Data storage

- Where is the data stored?
- Who has access to the data storage?
- What are the practices/processes/tools you are using to ensure the security of the storage device?
- Cloud storage vs physical storage vs device storage.

c) Data processing

- Who processes the data?
- Will the analysis of the data put individuals or groups at risk?
- What tools are being used to analyse the data?
- Who has access to the data analysis process/system?

- In the processing of data, are secondary copies of the data being stored elsewhere?

d) Publishing/sharing of information from the processed data

- Where is the information/knowledge being published?
- Will the publication of the information put people at risk?
- Who are the target audiences of the published information?
- Do you have control over how the information is being published?

e) Archiving

- Where is the data and processed information being archived?
- Is the raw data being archived or just the processed information?
- Who has access to the archive?
- What are the conditions of accessing the archive?

f) Deletion

- When is the data being purged?
- What are the conditions of deletion?
- How can we be sure that all copies are deleted?

Conclusion

This background document aims to help provide you with a conceptual overview of how to think about risk assessment from the perspective of movement organising. Often, risk assessment is done at the level of an individual, or an organisation. Thinking about this at the level of movements means asking participants to situate themselves as significant, yet partial, parts of a larger community of organisers.

This can be helpful as a common ground for groups of people who are organised differently to come together and think through a common plan, when a shared context, aim or activity is identified. It can also help to facilitate processes for collective thinking around sustainability and organising by anticipating and planning for risks related to group and relational dynamics, and

where information and communications technologies play a critical role as movement infrastructure.

You can share this as an additional resource for background reading with participants, or choose specific layers to further deepen as a group exercise or discussion.

Further reading

More broadly on understanding movement building and collective organising, as well as on digital realities:

- ICTs for Feminist Movement Building: Activist Toolkit: https://genderit.org/resources/icts-feminist-movement-building-activist-toolkit
- Making a Feminist Internet: Movement building in a digital age: https://www.genderit.org/editorial/making-feminist-internet-movement-building-digital-age
- Achieving Transformative Feminist Leadership: A Toolkit for Organisations and Movements: https://www.sexualrightsinitiative.org/resources/achieving-transformative-feminist-leadership-toolkit-organisations-and-movements

image-1605451259399.png

Revision #7
Created 18 April 2023 04:44:12 by Kira
Updated 28 July 2023 14:51:36 by Kira