Threat Models and Protest Security Specific Takeaways for Pro-Palestine Protesters

Updated October 2025

Introduction

We are members of a progressive tech working group in the Boston area. Our main project is the infosecforactivists.org website.

Questions:

- How does your group make decisions?
- How do you decide who to trust?
- Any pre-existing group agreements? How have you handled infosec up till now?

Learning goals

By the end of this session, you should be able to:

- Identify traits of good and bad security culture
- Explain what a threat model is
- Discuss the security culture your group has and wants
- Start thinking about a threat model for your situation

This short workshop is meant to introduce you to the concepts of **Security Culture** and **Threat Models.** It will also offer specific measures to counteract the threats faced by pro-Palestine protesters in the Boston area.

- **Security Culture**: A mindset shared across a group, meant to protect members of that group from outside threats
- **Threat Model**: A list of specific threats faced by a group/organization, so that the group can take specific measures to counteract them

Good Security Culture

Security, like gender, is a spectrum. Most people talk about it as a binary, and we always cringe when we hear activists talk about a service or practice being “secure” or “not secure.” However, in reality, what may be secure in one setting may not be secure in another.

What may be a secure practice in one situation may be insecure in another, or could be compromised by strategies you're not aware of. For example, many anonymous chat apps can still view your IP address, and can be tied back to your real identity unless you take further measures like using a VPN. Even if a chat app company doesn't store your messages in their systems, someone could still physically take your own device and look at your messages there.

Best practices also depend heavily on your digital, physical, legal, and emotional capabilities.

Security always involves tradeoffs between privacy and convenience. A complicated security routine may be secure so long as it is followed to the letter, but may be too complex for most people to follow *precisely*, leaving weak links in your group, or may be too complex to follow in the heightened emotional state of an imminent danger, failing exactly when you need it most. **Think of this from a harm reduction standpoint.**

Here are some examples of tradeoffs between security and convenience:

- Deleting social media would make us more secure, but it's probably not realistic since many people's livelihoods and personal connections rely on it.
- It's best not to use navigation apps like Google Maps to get to a protest location, but without one you may get lost on the way.
- Deleting all our text messages every day would be more secure, but then it would be more challenging to remember what plans were made.
- Having discussions only in person (rather than over text message) is more secure, but it's much less time-efficient.

What other tradeoffs can you think of?

A healthy security culture will make it easier for your group to do the work you've chosen, not harder.

Good security culture is also a culture of consent. If a member of the group attempts to pressure others into measures they aren't comfortable taking, those measures are going to fail.

It's crucial to understand the most important threats to your group so you can decide which practices are most important to achieve your goals. Just like in any aspect of organization, keeping your shared goals in mind will help you through moments of conflict around security.

Bad Security Culture

What can that look like?

Bad security culture is imprecise.

It often arises from the demands of a minority of group members (rather than the consent of the group).

If it has a threat model, it's either overblown (e.g. hiding from police or even federal authorities for perfectly legal work) or focused on only one pillar of security culture (e.g. demanding that group members adopt a onerous routine that exhausts them, draining them even before the actual activism has started).

Bad security culture emphasizes fearmongering, and castigates individual members of the group for their perceived failures, rather than using shared threats to build community and strengthen bonds between members.

Threat Modeling

Good threat models are the basis of good security culture. Knowing the specific threats faced by your group will help you create a culture of security that mitigates the risks to your group, but does not restrict the work you're attempting to do.

When we have given this training in the past, activists were being doxxed and harassed by counterprotestors. They were not sure how the counterprotesters were learning their identities, but wanted to make it stop. (This turned out to be the publicly available facial recognition platform "PimEyes.")

What threats are your group most concerned with at this time?

(Brainstorm/popcorn)

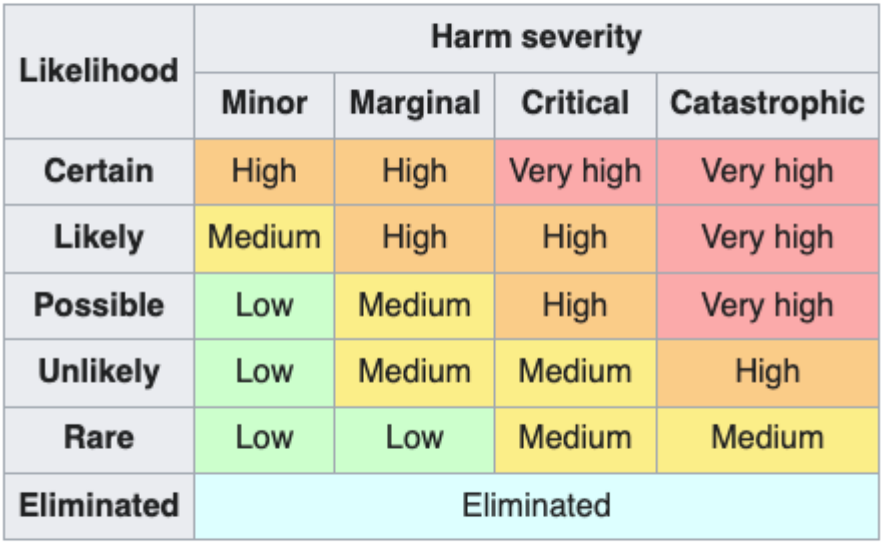
Some types of threats you may face include:

- Physical
- Emotional
- Legal
- Digital

Once you have identified threats, you will need to assess:

- How **likely** the threat is to happen
- How **severe** the consequences of the threat are

One tool for assessing risk using these criteria is a "Risk Matrix": https://en.wikipedia.org/wiki/Risk_matrix



Likelihood	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

(screenshot from Wikipedia)

Place the threats you identified in a risk matrix of your creation. It doesn't need to look exactly like the one in the screenshot - create one that suits your needs.

Case Study: Good Security Plan Example

Here is an example security plan for a pro-Palestine protest group in Boston from 2023.

This group's actions are legal, so they are not at risk of legal consequences (again, the year is 2023). However, they still face harassment pro-Israel factions in the Boston area who show up to counterprotest. The pro-Israel faction seeks to identify the personal information from pro-Palestine protestors, so they can subject them to IRL harassment, as well as online stalking and harassment campaigns branding them as “antisemites” to intimidate them and subject them to personal and professional consequences.

When we first offered this presentation, July 9, 2024, the pro-Israel faction in Boston had identified several pro-Palestine protesters. They appeared to know their names, but not much else about them, which suggested that the pro-Israel faction had access to a commercially available facial recognition database, most likely PimEyes, rather than a dedicated intelligence team.

Knowing this, the pro-Palestine group decided to hold a session and have their members remove themselves from PimEyes results using the following tutorial: https://pimeyes.com/en/tutorials/how-to-remove-your-images-from-pimeyes-search-results

Additionally, while the pro-Israel forces have not yet escalated to protesting the homes or workplaces of pro-Palestine activists, they plan for this eventuality, and decide to help their members remove their "Personal Identifying Information" such as their phone number, email, and address from online data brokers. While the group could use a commercial service such as DeleteMe or Optery, the cost of those services (approximately $150/year) is beyond the means of some members of the group. Instead, they decide to hold a group session where members can help each other manually removing those entries by following the steps in this guide: https://inteltechniques.com/workbook.html

Threat model:

- ***Personal information is being compromised*** *by the pro-Israel faction finding individuals in the group on the facial recognition service "Pimeyes"*
- *Group members may be targeted for* **protest at their homes or workplaces** *in the future*
- *Group members are being targeted for* **harassment on personal social media**
- *Group members are being targeted for* **harassment on LinkedIn***, potentially leading to career and financial consequences*

They start by removing members' results from the most prominent online peoplesearch engines and then work on others as they appear in the Google results for each member's name. This serves to not only protect the digital security of the group, but create a cohesive ethos of security among the group.

Additionally, they all agree to a few ground rules:

- *Don't post pictures of pro-Palestine protesters online (or tag them in status updates) without their consent,*
- *Don't post inflammatory statements online that could leave them (and the group) open to accusations of antisemitism.*

To protect their identities from IRL identification by the opposition, the group agrees to wear N95 masks at public events, and to refrain from using real names at public events.

The group also agrees to communicate about actions only via Signal, and agree that adding someone to the Signal group requires the consent of the group, via a "silent procedure." In this procedure, once a new member is nominated to be added to the Signal chat, the rest of the group has 24 hours to state their objections before that member is added.

Security practices:

- *Remove personal information from publicly available services*
- *Stop posting images of and tagging protestors on social media unless consent is given*
- *Wear N95 masks at public events*
- *Refrain from using real names at public events*
- *Only use a group chat on Signal to communicate about actions*
- *Only add a new member to the Signal chat after others have had 24 hours to object*

Security culture:

- *The group uses the **decision-making processes that work for them** to choose which security practices to put in place*
- *The group chooses practices that **address the threats they identified***
- *The group chooses practices that are **not too burdensome to follow consistently***
- *Members of the group **help one another** follow the practices they agreed on*
- *A **shared understanding** of their threat model and the kind of security culture they want prepares them to handle unknown dangers in the future*

Case Study: Bad Security Plan Example

Bad security culture vastly overemphasizes security practices and ignores the need for those practices to be practical to follow. It also shuts down communication from group members for whom the security practices are too cumbersome. Some possible outcomes of this culture are:

- The group becomes less secure, as everyone lies about whether or not they are following the agreed-upon practices. In the worst case, not listening to members who are struggling to follow security practices can result in security being breached in ways that hurt group members.
- The group shrinks, as people leave the group due to its security practices rendering the group ineffective (or just unpleasant)

Some real groups' security guides forbid their members from:

- Having social media
- Contacting other members by phone
- Hanging out at each others' houses
- Discussing their personal lives in the chat
- Disclosing their politics in real life-- even to friends or family

Though this security plan is comprehensive, it's so restrictive that it inhibits organizing and retention.

Most people-- especially those 18-30-- use social media obsessively. It's how they connect with others in their community, so telling them not to do this just makes them ignore the advice completely, rather than adapt it to suit their needs. (This is why we encourage thinking about threat models rather than a simple binary checklist of "secure/not secure.")

Despite national media coverage and years of consistent stickering, the group has failed to grow their membership, create a broader social climate for their far-right views, broaden their activism beyond stickering, or (with one notable exception, a 2018 attack on an ICE occupation in Texas) significantly disrupt any leftist organizing.

In other words, Patriot Front are shooting themselves in the dicks, over and over. Their threat model only includes the threat that getting doxxed would present to individuals, not the damage that their security plan is doing to their work and their organization.

Patriot Front's security protocols-- while marginally increasing the security of their organization-- appear to be inhibiting the work that they do as an organization, which is the exact opposite of what security protocols are supposed to do.

Main Takeaways

What are your main takeaways?

- **Don't talk to the police.**
- **When in doubt, don't put anything political online.**
- **Set your LinkedIn to private**: Pro-Israel protesters target the employment and professional affiliations of pro-Palestine protesters they are able to identify.
- **Don't use your real name online.** Don't post about protests on social media.
- **Wear masks at protests**: Wearing a mask not only supports public safety, but will defeat most facial recognition software
- **Assess threats**: Consider what poses the greatest danger to your group and its work.

Scan to download a PDF of this document

https://infosecforactivists.org/documents/
threat-models-and-security.pdf