Infiltration Prevention Toolkit

Protocols for Detecting Threats, Maintaining Trust, and Securing Resistance Spaces

TRANS ARMY

Last update: 2025-04-30

Infiltration Prevention Toolkit

Protocols for Detecting Threats, Maintaining Trust, and Securing Resistance Spaces

Version 1.4 – April 2025

Infiltration is no longer rare, it's expected.

As of 2025, state and far-right actors rely on infiltration as a primary tool to dismantle movements. Undercover cops, fascist saboteurs, and self-serving opportunists are already inside your chatrooms, signal chains, protest pods, and community kitchens.

But **paranoia is not strategy**. This guide equips you to **resist infiltration without turning on each other**.

It's a survival doctrine for radical spaces: how to verify new members, detect manipulation, and maintain community strength without replicating carceral suspicion. It's not about trustlessness. It's about **precision care**.

Inside, you'll find:

- Current infiltration tactics used by cops, fascists, and bad-faith actors
- Anti-infiltration protocols for digital, IRL, and internal culture
- Vetting processes, red flags, and layered access strategies
- Tips for digital hygiene, social engineering detection, and threat modeling
- Conflict vs. infiltration: how to call in without collapsing trust
- Tools, zines, and encrypted platforms that resist surveillance

This guide keeps your crew alive by teaching you **how to gatekeep the right way**.

🕵️ Common Infiltration Tactics (2022–2025 Trends)

🔍 Law Enforcement

- Undercover cops joining protest orgs, Discord servers, housing collectives
- Use of snitches + CIs (confidential informants) threatened with legal charges
- LARPing as radicals to incite illegal activity for entrapment

🦠 Far-Right Operatives

- Gaining admin access to chats, doxxing members, leaking plans
- False flag attacks or calls to escalate violence to discredit groups
- Targeting specific people with harassment campaigns after gaining trust

🧊 Internal Threats

- Burnout-induced disclosure
- "Tourist" organizers sharing plans or identities online
- Conflicts that go unresolved and create exploitable divisions

🧠 Core Principles of Infiltration Defense

- **Trust is built, not assumed**: Never skip the slow work of vetting
- **Security culture is culture**: Make it normal, not exceptional
- **Decentralize and compartmentalize**: Nobody needs access to everything
- **Normalize refusal**: "No" is safety, not drama
- **Disrupt charisma traps**: Leaders are roles, not people

🧰 Practical Anti-Infiltration Measures

🔐 Digital

- Use **Signal/Session/Briar** for all high-risk chats
- Never post organizing details on public or semi-public platforms
- Verify identities in multiple ways (voice + in-person + shared contacts)
- Rotate access: Don't give long-term admin power to one person
- Treat Google Docs as surveillance devices—host secure docs offline

🧭 IRL

- Never allow new people into sensitive spaces without a process
- Ask gently: who do they know? What have they done? Where are they based?
- "Three touch" rule: new people need multiple vouches from multiple pods
- Use entry-level events (teach-ins, training, kitchen work) to test reliability

💉 Internal Practices

- Run **conflict transformation pods** to prevent splintering
- Train members in **social engineering detection** and **OpSec basics**
- Host quarterly **threat modeling** meetups: review leaks, risks, plans

🔥 Red Flags for Potential Infiltrators

- **Refusing to share any personal details over long periods**
- **Overeager for action without doing base work**
- **Encouraging violent escalation without community discussion**
- **Always pushing for urgency, secrecy, or skipping process**
- **Weaponizing identity to avoid accountability**

🤝 Conflict vs. Infiltration

Not all disagreement is infiltration. Distinguish between:

- **Disagreement**: Good-faith critique
- **Disruption**: Repeated derailment, especially in critical moments
- **Deception**: Lying about affiliations, planting rumors, hoarding access

Build internal accountability systems so that *calling in* doesn't automatically become *calling out*.

📦 Tools & Resources

- **Zines**: "Security Culture 101," "How to Spot an Infiltrator," "Operational Security for Queer Rebels"
- **Workshops**: Blue Ridge Anarchist Skillshare, Radical Resilience, Antifa Self-Defense Clinics
- **Digital**: SimpleX, CryptPad, Riseup Pads, Qubes OS, OpenPGP

Conclusion

You can't stop every infiltrator.
But you can stop them from doing damage.

Resilient movements don't rely on paranoia.
They rely on **consistency, clarity, and refusal to collapse under fear**.

Security is not about gatekeeping power.
It's about protecting the people you fight beside.

Trust slow. Move smart. Stay sharp.