Deception Toolkit

Disinformation, Ghost Networks, and Camouflage Strategy for Trans-Led Information Warfare

TRANS ARMY

Last update: 2025-05-06

Deception Toolkit

Disinformation, Ghost Networks, and Camouflage Strategy for Trans-Led Information Warfare

Version 1.3 – April 2025

The **Trans Army Deception Toolkit** is your doctrine for confusion-based resistance: a guide to filling surveillance feeds with fog, exhausting state actors, and creating ghost trails to protect your real comrades and networks. Misinformation here is a **defense technology**, not a game, not a prank, but a discipline.

This guide draws from real-world decoy ops, case studies in misdirection, and decades of asymmetric strategy. It centers **ethics**, operational containment, and clarity of purpose: protect the vulnerable, disrupt the oppressive, and waste the enemy's time.

Inside you'll learn:

- How to launch fake protest plans, ghost cells, and burner campaigns
- How to use metadata traps and spoof accounts for counter-doxxing
- Tools for flooding digital intel pipelines with misdirection
- Protocols to keep real ops insulated while decoys run hot
- Examples of field-tested tactics from 2024–2025 queer resistance ops
- Ethical hard lines: what we never do, even to the enemy

This isn't chaos.
This is disciplined defiance.

⚠️ Tactical Overview

In asymmetric conflict, deception is a force multiplier. When used strategically and ethically, **controlled infiltration and misinformation** can buy time, mislead hostile actors, waste state resources, and reroute repression. This guide provides principles and tactics for using misinformation and *false positive infiltration* against oppressive systems, without endangering comrades or communities.

Note: These tactics are for information warfare. Never use deception to frame, endanger, or expose real individuals. This is strategic misdirection, not scapegoating.

I. Strategic Objectives

1. **Saturate state intel systems** with false leads
2. **Waste resources** of police, fascists, and surveillance agents
3. **Delay crackdowns** by flooding targets with decoys
4. **Protect real networks** by creating "noise clouds"
5. **Build digital camouflage** to blur or obscure high-value targets

II. False Identity Tactics

1. Ghost Operatives

- Create fake radical accounts that engage in exaggerated, non-actionable rhetoric
- Use them to draw surveillance away from real planning spaces
- Seed them with "bad ops" that the state may waste time investigating

2. Decoy Cells

- Organize publicly visible "groups" that never meet in person
- Make them loud, visible, but structurally empty
- Use them to absorb infiltrators, media attention, or event permits

3. Tactical Leaks

- Leak real-sounding but entirely fake protest plans, routes, or targets
- Use burner accounts on known surveillance platforms (Facebook, Instagram, Telegram)
- Schedule "events" that drain police resources without endangering anyone

III. Digital Misinformation Tactics

1. Data Pollution

- Use bots, spoofed devices, and duplicated usernames to inflate or distort organizing metrics
- Mirror real movements with small changes in taglines or icons
- Link fake pages to state officials to create false intel trails

2. Surveillance Trap Rooms

- Create fake Signal groups with bait conversations
- Leak the invite links into right-wing or law enforcement channels
- Monitor access, plant misinformation, then shut down

3. Counter-Doxxing Bait

- Upload fake name lists or "leaked docs" with booby-trapped data
- Track who downloads or spreads them
- Use metadata tracing to identify bad actors

4. Operational Rules

- Always silo ops: no one person runs both real and decoy networks
- Use automation + air gaps, never run from your real devices
- Never claim false flags publicly, maintain ambiguity
- Always have escape paths for mistaken identity or exposure

IV. Ethical Boundaries

✅ Allowed:

- Fooling cops, fascists, corporations, or feds
- Creating decoys to protect real people
- Misleading surveillance AI with plausible noise

❌ Forbidden:

- Framing real people or orgs
- Endangering vulnerable groups with fake info
- Amplifying fascist disinformation under the guise of infiltration

V. Tools of the Trade

- **Burner devices** w/ GrapheneOS or Tails
- **Bots** (Telegram, Discord, Twitter) for automation
- **Metadata erasers** (ExifTool, MAT2)
- **Open-source face generator** tools (ThisPersonDoesNotExist)
- **Dummy form fillers + fake contact networks**

VI. Example Scenarios (2024–2025)

- Atlanta organizers created decoy permit apps for Cop City to delay surveillance sweeps
- LA activists ran spoof networks mimicking a known queer housing collective, leading Proud Boys to the wrong location
- Mutual aid groups used fake protest route leaks to avoid preemptive kettling during Pride weekend

Conclusion

Misinformation is an artform when deployed with ethics and precision. Our enemies rely on prediction and surveillance. Confuse them. Waste their time. Cloud their tools.