Counter-Surveillance Tactics

Evading Machines, Disrupting Profiles, and Moving Unseen in a Tracked World

TRANS ARMY

Last update: 2025-05-06

Counter-Surveillance Tactics

Evading Machines, Disrupting Profiles, and Moving Unseen in a Tracked World

Version 1.2 – April 2025

In 2025, surveillance is no longer speculative. It's tactical. Facial recognition systems scrape your selfies. Predictive policing maps your movements. Social platforms act as informants. Cops use drones, AI, and license plate readers in real time. The machine doesn't just watch, it hunts.

This field guide is a **countermeasure**.

It teaches you to **disrupt inputs**, **jam signals**, **mislead metadata**, and **break the automation of profiling**. It teaches you to survive a world that thinks it already knows who you are.

This is not about disappearing. It's about becoming **unreadable**. It's about building ghosts, trans, disabled, neurodivergent, undocumented, and otherwise targeted folks who refuse to be rendered visible by a system built to cage them.

Inside you'll learn:

- How to confuse facial recognition with layering, patterns, and IR gear
- How to reroute around surveillance infrastructure using open tools
- How to build and maintain digital hygiene across multiple ops
- How to train your body to move unpredictably and quietly
- How to build a security culture inside cells, not just around them

You don't need to vanish. You just need to be noise.
Become unreadable. Stay moving. Outlast the machine.

⚠️ Why Counter-Surveillance?

In 2025, surveillance is the state's primary weapon of control. Facial recognition, predictive policing, AI-enhanced tracking, and digital infiltration have turned everyday life into a panopticon. This guide outlines how to resist, confuse, evade, and disrupt surveillance systems targeting movements, communities, and individuals.

I. Who's Watching?

Surveillance in 2025 isn't just a government operation anymore. It's a sprawling, interoperable mesh of state agencies, corporate algorithms, and private extremist networks, all watching, collecting, and cross-referencing. Especially for trans people, leftist organizers, sex workers, and mutual aid networks, this ecosystem operates more like a counterinsurgency occupation than mere oversight.

1. State Surveillance

Agencies Involved:

- DHS (Department of Homeland Security): Flagging activist language, monitoring trans-border movement, running keyword flag systems.
- FBI (Federal Bureau of Investigation): Scraping Signal metadata, compiling activist watchlists, embedding informants.
- Fusion Centers: Regional intel hubs where federal, local, and private-sector surveillance converge, massively underregulated.
- ICE: Monitors and cross-checks DMV, employment, housing, and even school data to hunt undocumented and trans asylum seekers.
- State-level anti-trans task forces: Often created by executive order; share data with national partners.

Key Tactics:

- Keyword and image flagging on open platforms (especially TikTok, Twitter, YouTube).
- Geofencing protests and pride events.
- Scraping encrypted traffic volume (not content) for pattern detection.
- Use of facial recognition at airports and highways.
- Deployment of stingrays (fake cell towers) at rallies and drag events.

2. Corporate Surveillance

Core Players:

- Data Brokers: Acxiom, Oracle, LexisNexis sell personal profiles including HRT prescriptions, browsing habits, and gender marker changes.
- Facial Recognition Retail Networks: Walmart, Walgreens, CVS quietly use AI-based theft prevention that logs biometric patterns.
- Social Media Giants: Meta, TikTok, and X (formerly Twitter) share access with law enforcement, censor protest hashtags, or deprioritize "flagged" accounts.
- HealthTech & AdTech Collusion: Apps like period trackers, health monitors, and even Uber collect gendered movement patterns.

Key Tactics:

- Location tracking via apps, even when “off.”
- Advertising algorithms that reinforce gender conformity, political paranoia.
- De-anonymizing burner phones through app syncs and MAC address mapping.
- Geo-marketing campaigns that mirror police surveillance zones.

3. Private Fascist Networks

Who Are They:

- Telegram fascist channels
- 4chan/8kun cells
- Local far-right militias
- Online doxxing coalitions like LibsOfTikTok and Moms for Liberty

What They Do:

- Scrape social media for school staff, organizers, and trans people to doxx and harass.
- Organize bounty-style systems in red states (TX, FL, MO) to report parents of trans kids, drag performers, or HRT users.
- Map and circulate "gender-ideology hot zones" using scraped images, event calendars, and AI-driven face matching.

Tech Used:

- Publicly available datasets + AI facial clustering.
- Botnets for mass harassment.
- FOIA requests turned into intimidation tools.

III. Key Surveillance Technologies in 2025

In 2025, surveillance is no longer siloed, it's fully integrated across public, private, and rogue networks. These technologies don't simply observe; they form a multilayered system of **predictive profiling, behavioral nudging, and automated enforcement.**

State agencies deploy AI and drones, corporations track every click and step, and fascist groups scrape and doxx from the sidelines. Together, they form a **360° threat ecosystem** where your face, car, gait, voice, and digital shadow can all become flags in a database.

This section dissects the core technologies fueling this apparatus, what they are, who controls them, how they're used, and why they're dangerous. Learning the tools is the first step toward jamming them.

1. AI Facial Recognition

Core Systems:

- **Clearview AI**: Scrapes billions of public images (social media, press, surveillance feeds) to match faces.
- **Amazon Rekognition**: Powers many law enforcement and private retail systems across the U.S.

Real-World Uses:

- Tracking protest attendance in real-time.
- Retroactive arrests using tagged photos from social media.
- "Watchlist" matching in airports, schools, and hospitals.

Risks:

- High false-positive rates for BIPOC and trans faces.
- Used by private companies without consent.
- Nearly impossible to opt out of once scraped.

2. License Plate Readers (ALPR)

How They Work:

- Stationary or vehicle-mounted cameras that scan plates and log date, time, GPS.
- Synced with national law enforcement and private databases.

Operators:

- Police departments
- Towing companies
- Neighborhood associations

Uses:

- Flagging cars near activist homes or events.
- Tracking travel patterns across state lines.
- Partnered with ICE for immigration enforcement.

3. IMSI Catchers ("Stingrays")

What They Do:

- Mimic a real cell tower to trick your phone into connecting.
- Capture location, metadata, and sometimes content.

Deployed By:

- Federal agents (FBI, DHS)
- Local cops with federal funding

Known Deployment Zones:

- Protest sites
- Border towns
- Urban queer spaces and public transit hubs

4. Smart Camera Networks

Systems in Use:

- **Ring (Amazon)**: Video doorbells and neighborhood watch networks.
- **Flock Safety**: Neighborhood license plate and motion cameras.
- **Traffic and city surveillance feeds**: Often patched into police fusion centers.

Risk Factors:

- Private users sharing footage with cops without warrants.
- Facial and license plate scanning baked into firmware.
- Often backed by "neighborhood safety" apps with vigilante tendencies.

5. Drone & Aerial Surveillance

Capabilities:

- Thermal imaging (can see through tents, brush, some walls)
- Live audio pickup and high-zoom visuals
- Geofencing and automated pathing

Common Operators:

- Customs and Border Patrol
- Local police at protests
- Private security firms protecting pipelines, prisons, etc.

Implications:

- Used to "kettle" protestors
- Scan queer encampments or houseless hubs
- Harass undocumented or T4T mutual aid groups

6. Predictive Policing Software

Systems:

- **ShotSpotter**: Uses AI microphones to detect gunshots (but misfires often)
- **Palantir Gotham**: Aggregates criminal, personal, financial, and location data to flag "pre-crime" suspects
- **PredPol**: Tells cops where to patrol based on past data (usually just reinforces racist policing)

Dangers:

- Used to justify harassment of people "likely to offend"
- Targets entire neighborhoods based on biased arrest data
- Invisible to the public and nearly impossible to challenge legally

IV. Tactical Counter-Surveillance

This section is for anyone who needs to walk through a city unseen, vanish from a drone's scope, or scramble the eyes of the machine. Counter-surveillance isn't about becoming a ghost, it's about being a glitch in the system. It's about turning every algorithm into a liar and every cop into a fool chasing shadows.

We outline practical, field-tested methods for blocking facial recognition, jamming vehicle tracking, and making surveillance tech work against itself. These tactics are pulled from the playbooks of street medics, direct action crews, T4T survival networks, and antifascist organizers operating under real-world threat.

You'll find wearable tech tricks, vehicle masking tips, and modular obfuscation strategies for protests, evasion, and everyday dissent. Whether you're dodging facial scans or building mobile cover squads, these practices are meant to be shared, adapted, and spread.

This is how we blur the face of empire. This is how we walk free when freedom is denied.
Stay mobile. Stay masked. Stay ungovernable.

1. Visual Disruption (Facial Recognition)

Masks + Layering

- Combo of **mask + glasses + hat** significantly alters AI facial profile.
- Aim to shift **head shape**, **jawline visibility**, and **eye recognition** points.
- Change colors, shapes, and angles frequently.

Infrared (IR) LED Wearables

- IR LEDs (invisible to human eyes) can flood surveillance cams.
- Embedded in hats, necklaces, or glasses.
- DIY versions available with LED strips + battery pack + 940nm IR bulbs.

Reflective Materials

- Use foil stripes, chrome stickers, and mirrored accessories.
- Reflects light back into the lens, overexposing the image.

Makeup Camouflage (CV Dazzle)

- Use **asymmetrical, high-contrast makeup** patterns.
- Target AI fiducial points (eyes, nose, mouth) to cause misreads.
- Combine with wigs and prosthetics for total profile obfuscation.

Adversarial Clothing

- Shirts, hoodies, or scarves printed with "fake faces" confuse facial AI.
- QR codes, nonsense barcodes, or fake eyes also jam detection.
- Some designers offer adversarial fashion kits (check underground T4T vendors).

2. Vehicle & Transit Obfuscation

Plate Evasion Tools

- **Plate covers** (clear or tinted) can block upward angles. *Illegal in most states.*
- **Reflective sprays**: Apply over characters to bounce back ALPR light.
- **Decoy plates**: Magnetic overlays or mud coatings during actions.

Rerouting Strategies

- Avoid known ALPR/shotspotter intersections. Use **OpenStreetMap + OSMAnd** with overlay plugins.
- Install **Surveillance Outreach** extensions to check known camera zones.

Alternative Mobility

- Use **bicycles, e-scooters**, or **on-foot paths** through alleyways and trails.
- Carpool with friends using **offline GPS and analog maps**.
- Avoid **ride-share apps** when engaging in direct actions. Use community ride boards or burner numbers.

V. Digital Hygiene

In a world where surveillance is ambient and data trails are weapons, digital hygiene isn't optional, it's insurgent self-defense. This section is a tactical toolkit for anyone operating in or adjacent to high-risk environments: queer organizers, street medics, hacktivists, trans anarchists, whistleblowers, and everyday people who refuse to be cataloged, indexed, or sold.

We break down tools and practices into bite-sized, usable categories: what to carry, how to communicate, where to browse, and how to host your content. Every section is field-ready and field-tested, built from direct experience dodging corporate spyware, state dragnet tools, and right-wing doxxing networks.

Digital hygiene is not about being perfect. It's about making yourself unpredictable, too expensive to monitor, and too encrypted to exploit. It's about being ungovernable *even through your metadata.*

Build your stack. Rotate your keys. Mask up, online, too.

1. Devices

Burner Phones

- **Buy with cash only.** Never use cards, never activate in your name.
- Keep **physical separation** from your daily-use phone. Never carry both together.
- Use only for one operation or contact chain, then retire it or factory reset and repurpose.

Faraday Bags

- Blocks GPS, cell, Wi-Fi, and Bluetooth signals.
- Use when in transit to evade location logging.
- Make sure bag seals are tight; check signal with a second device.

Secure Operating Systems

- **Tails OS**: Live boot OS that leaves no trace. Best used on public or shared machines.
- **GrapheneOS**: Hardened Android fork; ideal for repurposed Pixel phones.
- **Qubes OS**: For compartmentalized desktop opsec (advanced users).

2. Communication

Encrypted Apps

- **Signal**: Best overall, with disappearing messages and verified safety numbers.
- **Session**: Anonymous routing without phone number. Good for burner ops.
- **Briar**: Mesh-based, works even without internet (great for field operations).

Platform Avoidance

- **No Google, Facebook, WhatsApp, Instagram, or Gmail** for sensitive comms.
- These platforms leak metadata, log content, and share with LEAs on request.

Account Rotation

- Each new operation or network = new account, new username, new email.
- Use alias generation tools to maintain plausible identities.
- Rotate contact trees, never keep the same people in all ops.

3. Browsing & Data Practices

Tor Browser

- Use for all political, research, or risky queries.
- Always check you're on **https**.
- Don't use personal logins while on Tor.

Zero Trace Habits

- Disable autofill, location, camera, and microphone.
- Use **incognito mode + cookie blocker + fingerprint randomizer**.
- Never reuse passwords. Use air-gapped password vaults or paper backup stored offsite.

Radical Hosting

- Host docs on decentralized tools:
    - **Onion services** (Tor hidden sites)
    - **IPFS** (InterPlanetary File System)
    - **ZeroNet** (anonymous peer-to-peer web)
- Encrypt documents before upload. Use PGP or VeraCrypt.

4. Behavioral Techniques

- **Vary your patterns**: Don't commute or message at the same time daily
- **Change appearance**: Simple shifts (hair, posture, gait) reduce pattern recognition
- **Misinformation layering**: Create noise profiles (fake interests, shadow accounts)
- **Cover devices when speaking**: Mics are always listening (AirPods, Alexa, phones)

VI. Physical Space Defense

This guide outlines practical, low-cost, and field-tested strategies for resisting surveillance and control in physical environments, urban and rural areas. It's built for trans mutual aid crews, street medics, resistance camps, direct action organizers, and anyone who needs to remain operational under threat from drones, cams, cops, or far-right militias. These tactics prioritize movement, misdirection, and terrain control rather than brute invisibility.

1. Urban Defense Tactics

Camera Disruption

- Use spray paint, posters, or laser pens to obscure or blind cameras.
- *Warning*: Legal only in permitted protest zones or if coordinated with legal observers.
- Covering or disabling private cameras can carry felony charges, know your local ordinances.

Mobile Cover Tools

- Umbrellas: Classic Hong Kong tactic. Use as cover for group actions or to block drone sightlines.
- Mirrored boards: Reflect light and confuse both cameras and facial recognition systems.
- Combine with coordinated movement for maximum screen effect.

Optical Interference

- Disco balls or mylar kites: Flood drone optics and camera sensors with unpredictable reflections.
- Bike spokes or window flashes: Carry spinning reflectors or solar lights to dazzle sensors.
- Reflective tape worn on limbs also helps mislead motion detection systems.

2. Rural & Perimeter Defense

Thermal & IR Evasion

- Foil-lined blankets, emergency bivvies, or heat-dispersing netting hide body heat.
- Build insulated dugouts with earth and thermal masks to avoid aerial IR.
- Keep movement low, slow, and layered to disperse heat signatures.

Controlled Burn Pits

- Use for burning ID tags, trace materials, and bio evidence.
- Dig small, coned pits lined with stones. Burn at dawn or dusk to minimize drone spotting.
- Mix with charcoal to mask chemical signatures from aerial sniffers.

Anti-Drone Terrain Tactics

- Set up netting canopies, tree cover, or use ruined buildings for air shield.
- Use chaff launchers (homemade from foil + compressed air) to confuse drone radar.
- Build false heat sources (e.g. decoy fires or hot water bottles) to throw off thermal cameras.

VII. Group Security Practices

Security Culture Is Mutual Survival. Security isn't just about protecting the mission; it's about keeping people alive. Building a **security culture** means developing shared norms, habits, and boundaries that reduce risk for everyone involved. It's not about paranoia. It's about predictability, accountability, and resilience.

1. Core Norms of Security Culture

Don't Talk About Crimes

- Don't ask. Don't brag. Don't speculate.
- Never talk about **illegal activities**, even hypothetically, in public or private spaces unless it's necessary for immediate survival.
- Assume every device and person is compromised until proven otherwise.

Don't Make People Liabilities

- Never pressure anyone to disclose past actions.
- Don't share someone else's identity, arrest history, trauma, or opsec level without their consent.
- Avoid social media hype that exposes others by accident (e.g. tagging locations, photos, or names).

Normalize "I don't need to know."

- Make refusal to know or disclose **a strength, not a weakness**.
- Practice saying: "I support what you're doing. I don't need to know the details."

2. Roles Within Secure Groups

Don't default to flat horizontalism or rigid hierarchy. Instead, create **rotating, role-based cells** with clear responsibilities but no permanent leadership structures.

Rotating Organizers

- Rotate visible spokespeople, organizers, and facilitators to prevent burnout and targeting.
- Build deep benches. Everyone should be trained to take over any task.

Avoid "Leader" Language

- Language creates vulnerabilities. Don't say "leader," "founder," or "head of."
- Use terms like **point**, **contact**, or **coordinator** to flatten perceived power.
- Keep public-facing roles vague and shared.

Specialized Roles

- **Digital Marshals**: Oversee encrypted tools, help with burner device setup, manage secure comms.
- **OpSec Officers**: Conduct internal audits, train new members, run threat assessments.
- **Infiltration Detectors**: Track inconsistencies, monitor entry patterns, and cross-reference stories.
- **Security Culture Keepers**: Normalize protocols, intervene in loose talk, maintain healthy paranoia.

3. Infiltration Defense

Trust Is a Process

- Vet people over time and across situations. Real comrades show up consistently, not perfectly.
- Don't trust anyone solely because they're queer, trans, or share your politics.

Watch for Red Flags

- Love bombing, oversharing trauma, excessive eagerness.
- Pushy behavior around strategy or illegal plans.
- Trying to isolate members or escalate internal drama.

Verification Tactics

- Cross-reference life stories through third parties.
- Google usernames, reverse image search photos.
- Test with "harmless bait" to see if info leaks.

4. Onboarding & Exit Protocols

New Member Onboarding

- Provide security culture training within first week.
- Offer guided access to secure platforms and document handling.
- Assign mentors for opsec coaching.

Exit With Dignity

- Create exit rituals that ensure **debrief, data wiping, and emotional closure**.
- Don't ghost people out of fear; give a respectful exit plan.
- Remove access to shared platforms or group data.

5. Accountability Without Carceral Logic

- Use **restorative and transformative justice** models for internal conflict.
- Avoid cancel culture vibes, public callouts can draw state attention.
- Focus on **harm reduction, repair, and consent-based reentry** to groups.

6. Other Practices to Consider

- **Decentralize access**: No one person should have the keys to everything.
- **Data minimization**: Don't collect what you don't need. Purge often.
- **Secure meetings**: Default to in-person with Faraday protocols, or encrypted voice only.
- **Opsec drills**: Simulate arrest, surveillance, or breach scenarios.
- **Mental health culture**: Burnout breaks security. Build in care from the start.

7. Tools: Physical & Digital Hardware

Obfuscator Browser Plugins

- **AdNauseam:** Clicks all ads in the background to pollute data profiles.
- **TrackMeNot:** Sends fake search queries to confuse profiling algorithms.
- **NoScript/uBlock** Origin: Block trackers, scripts, and cross-site cookies.
- **Privacy Badger (EFF):** Learns and blocks trackers over time.

SIM Card Duplicators / Cloaking Tools

- Used for SIM swapping, burner ID cloning, and disposable device use.
- Can clone old phones to new shells or create false logs.
- *Legal gray area*: Use only in high-risk activist scenarios.

Noise Jammers

- RF jammers block Bluetooth/WiFi for 5-10 meters.
- Used to break drone or smart camera feeds temporarily.
- Also jam microphones during private meetings.
- Portable voice scramblers (like ultrasonic jammers) interfere with acoustic sensors.

8. Apps for Field & Personal Security

Haven

- Turns any old smartphone into a motion, sound, and vibration detector.
- Great for safehouse perimeter alerts or shared mutual aid storage spots.
- Developed by Guardian Project + Edward Snowden.

Cryptomator

- Open-source client-side file encryption.
- Encrypts files *before* uploading to cloud services like Dropbox, GDrive.
- Cross-platform and mobile compatible.

Umbrella by Security First

- All-in-one mobile guide to digital and physical security.
- Includes training for protests, secure travel, and targeted surveillance response.
- Offline-capable, updated regularly.

Bonus Apps

- Jitsi Meet: Encrypted group video chat (host your own server for max security).
- CalyxOS/GrapheneOS: Privacy-focused mobile OS alternatives.
- Element (Matrix): End-to-end encrypted group chat platform.

9. Organizations & Networks

Tactical Tech

- Offers toolkits, workshops, and zines about data privacy, surveillance, and disinfo.
- "The Glass Room" project reveals how everyday tech spies on you.

EFF (Electronic Frontier Foundation)

- Legal advocacy + practical guides for staying private online.
- Creator of Privacy Badger, HTTPS Everywhere, and Surveillance Self-Defense.

Surveillance Self-Defense (by EFF)

- Comprehensive, no-jargon guide to privacy best practices.
- Customized tools for journalists, queer organizers, immigrants, and students.

Access Now

- Offers Digital Security Helpline 24/7 for activists under threat.
- Also fights internet shutdowns and anti-encryption laws globally.

Sudo Room / Sudo Mesh (Oakland)

- Radical tech co-op providing open infrastructure and free mesh internet.
- Supports community-run alternatives to Big Tech tools.

More to Follow:

- **Riseup.net**: Secure email, lists, pads, and VPNs for activists.
- **Tails / Qubes OS**: Secure, no-trace operating systems.
- **Collective Care Pods**: Peer groups training each other on opsec.
- **Library Freedom Project**: Teaching librarians digital resistance.

Conclusion

Surveillance in 2025 is not passive observation, it is extraction, prediction, and preemptive discipline. It targets movements before they grow, punishes deviance before it speaks, and maps lives before they become dangerous. But every system has limits, and every net can be jammed.

This guide isn't about fear. It's about fluency. About learning the language of your enemy so you can rewrite the script. For every camera, there's a blind spot. For every drone, a shadow. For every predictive model, a variable it can't understand.

You don't need to be invisible; you need to be unpredictable. You don't need to disappear forever; you need to reappear stronger. Let your movements blur, your data corrupt, your presence multiply.
We don't survive by shrinking. We survive by mutating.

Don't identify as a problem, be a problem, stay ungovernable.