THE ANALOG RESISTANCE TOOLKIT

HOW TO ORGANIZE WITHOUT DIGITAL SURVEILLANCE



A OPERATIONAL SECURITY WARNING

GREG WOLFORD



THE ANALOG RESISTANCE TOOLKIT

How to Organize Without Digital Surveillance A Complete Guide for Community Organizers

<u>∧</u> **OPERATIONAL SECURITY WARNING** This document contains sensitive information about surveillance-resistant organizing techniques. Handle with appropriate discretion. Print only when necessary. Do not store on networked devices.

TABLE OF CONTENTS

Chapter 1: Understanding the Surveillance State

Chapter 2: Ham Radio Networks for Resistance Communication

Chapter 3: Physical Dead Drop Systems

Chapter 4: Bulletin Board Intelligence Networks

Chapter 5: Cash-Based Mutual Aid Systems

Chapter 6: Counter-Surveillance for Organizers

Chapter 7: Emergency Communication Protocols

Chapter 8: The "Feed the Birds" Code System

Chapter 9: Building Analog Community Networks

Chapter 10: Legal Considerations and Safety Protocols

INTRODUCTION: WHY ANALOG RESISTANCE MATTERS

From the desk of the Underground Archive

In 2024, RakeTech CEO Emerson Rake admitted on underground radio that surveillance systems aren't just watching resistance activities - they're using them as training data.

Every encrypted message, every social media post, every digital organizing effort becomes information that helps authoritarian systems predict and suppress future resistance.

This toolkit provides practical alternatives developed by community organizers who've learned to operate below the digital radar. These aren't theoretical concepts - they're field-tested techniques being used right now by networks across the country.

The goal isn't to abandon technology entirely. It's to create organizing infrastructure that can't be mapped, predicted, or controlled by digital surveillance systems.

Remember: Strong communities don't need digital coordination. They need trust, relationships, and practical systems for mutual support.

CHAPTER 1: UNDERSTANDING THE SURVEILLANCE STATE

How Modern Surveillance Really Works

Digital surveillance isn't just about watching individual conversations. It's about **pattern recognition at scale**. Systems like RakeTech's behavioral prediction algorithms analyze:

- **Communication patterns:** Who talks to whom, when, and how often
- **Movement patterns:** Where people go, when they gather, how they travel
- **Financial patterns:** What people buy, where they spend money, resource flows
- **Social patterns:** Group formation, leadership emergence, influence networks

The Feedback Loop Problem

Traditional digital organizing creates a feedback loop:

- 1. Organizers use digital tools to coordinate
- 2. Surveillance systems learn from these patterns
- 3. Suppression tactics become more effective
- 4. Organizers adapt with new digital security measures
- 5. Surveillance systems learn from the adaptations
- 6. The cycle continues with increasing sophistication

Analog resistance breaks this cycle by operating outside the digital feedback loop entirely.

Key Principles of Analog Organizing

Principle 1: No Digital Footprints

If it doesn't exist digitally, it can't be tracked digitally.

Principle 2: Distributed Intelligence

Information flows through human networks, not data networks.

Principle 3: Physical Verification

Trust is built through face-to-face relationships and real-world actions.

Principle 4: Compartmentalized Operations

Each cell or group knows only what it needs to know.

Principle 5: Redundant Systems

Multiple backup methods for every critical function.

CHAPTER 2: HAM RADIO NETWORKS FOR RESISTANCE COMMUNICATION

Why Ham Radio Works

Ham radio operates on frequencies that require specialized equipment to monitor effectively. Unlike internet communications that pass through centralized infrastructure, ham radio is point-to-point or uses repeater networks operated by hobbyists.

Getting Started with Ham Radio

Step 1: Get Licensed

- Take the Technician Class exam (entry level)
- · Study guides available free online
- Local ham radio clubs often offer test sessions
- License is public record, but provides legal cover for radio activity

Step 2: Choose Equipment

- **Handheld radios:** Good for local communication (1-5 miles)
- **Mobile radios:** Vehicle-mounted, longer range (10-50 miles)
- **Base stations:** Home setups for maximum range and capability

Recommended beginner setup:

- Baofeng UV-5R handheld radio (\$25-35)
- Programming cable (\$10)
- Better antenna (\$20-30)
- Total investment: Under \$75

Resistance Communication Protocols

Protocol 1: Scheduled Check-ins

- Set regular times for network members to check in
- Use different frequencies on rotation
- Keep transmissions brief and coded

Protocol 2: Emergency Activation

- Designated emergency frequencies
- Code words for different types of alerts
- Relay procedures for spreading urgent information

Protocol 3: Information Verification

- Multiple sources required for important intelligence
- Chain of verification through trusted operators
- Time-stamping and source tracking

Basic Ham Radio Codes for Organizers

10-codes for resistance use:

- **10-1:** Signal weak / unclear
- **10-2:** Signal good
- **10-20:** Location (but never give real location)
- **10-33:** Emergency traffic (all others clear frequency)
- **10-99:** Stand by / stop transmitting

Phonetic Alphabet:

Alpha, Bravo, Charlie, Delta, Echo, Foxtrot, Golf, Hotel, India, Juliet, Kilo,
Lima, Mike, November, Oscar, Papa, Quebec, Romeo, Sierra, Tango, Uniform,
Victor, Whiskey, X-ray, Yankee, Zulu

Operational Security for Ham Radio

Do:

- Use call signs as required by law
- Keep political discussion off the air
- Focus on community service and emergency preparedness
- Join local emergency communication groups for credibility

Don't:

- Discuss specific organizing activities on air
- Use real names beyond required call sign identification
- Give specific locations or addresses
- Transmit encrypted messages (illegal for ham radio)

CHAPTER 3: PHYSICAL DEAD DROP SYSTEMS

What is a Dead Drop?

A dead drop is a method of spy tradecraft involving a secret location where information can be left by one person and retrieved by another without direct contact. For resistance organizing, dead drops allow information sharing without digital trails.

Selecting Dead Drop Locations

Ideal characteristics:

- **Public but not crowded:** Places people visit regularly but don't linger
- **Multiple access routes:** Easy to approach and leave from different directions
- **Natural concealment:** Locations where hidden items won't be discovered accidentally
- Regular maintenance: Places that are cleaned or maintained, but not obsessively
- Plausible reasons to visit: Locations where your presence seems normal

Good dead drop locations:

- Library book sections (tape envelope inside rarely-used books)
- Public park bulletin boards (behind posted flyers)
- Community center restrooms (behind toilet tanks)
- Church or community building common areas
- 24-hour laundromats
- University campus study areas

Avoid:

- High-security locations with cameras
- Places with metal detectors or security screening
- Locations that require ID or registration to access
- Anywhere with predictable cleaning schedules
- Your own neighborhood or frequently visited areas

Dead Drop Protocols

Protocol 1: Signal System

- Load signal: Indication that information has been placed
- **Clear signal:** Indication that information has been retrieved
- **Danger signal:** Warning that location may be compromised

Example: Chalk marks on specific utility poles, or arranged items in public spaces

Protocol 2: Timing

- Set specific windows for deposits and retrievals
- Never visit the same location twice in one day
- Vary your schedule and approach routes
- Use the "three-day rule" if information isn't retrieved within 72 hours, assume compromise

Protocol 3: Information Security

- Never put names or identifying information in dead drops
- Use code words and reference numbers
- Include date/time stamps for time-sensitive information
- Write in generic handwriting or use typewriter/printer

Dead Drop Materials and Concealment

Waterproof containers:

- Small zipper bags
- Film canisters (if you can find them)
- Pill bottles
- Magnetic key holders for metal surfaces

Concealment methods:

- Tape items behind permanent fixtures
- Hide in hollow spaces (railings, fence posts)
- Camouflage among existing posted materials
- Use magnetic containers on metal surfaces
- Bury in parks or wooded areas (mark location discretely)

CHAPTER 4: BULLETIN BOARD INTELLIGENCE NETWORKS

Why Physical Bulletin Boards Work

Community bulletin boards exist in most neighborhoods and are regularly checked by locals. They provide a way to distribute information to large numbers of people without individual targeting or digital tracking.

Locations for Information Distribution

Community spaces:

- Coffee shops and cafes
- Community centers

- Libraries
- Grocery stores
- Laundromats
- Churches and religious centers
- University campuses
- Community gardens

Public spaces:

- Park bulletin boards
- Transit stops (where posting is legal)
- Community event spaces
- Farmers markets
- Neighborhood associations

Information Distribution Techniques

Technique 1: Layered Information

- Post innocuous community information on top
- Include resistance information in layers below
- People naturally peel back layers to see what's underneath

Technique 2: Contact Numbers

- Post tear-off tabs with phone numbers
- Use burner phones or voice-only services
- Change numbers regularly
- Include coded information in the numbers themselves

Technique 3: QR Codes

- Create QR codes linking to resistance information
- Host content on secure, anonymous platforms
- Include QR codes in legitimate-looking flyers
- Change target URLs regularly

Technique 4: Event Announcements

- Announce legitimate community events
- Include coded information about actual meetings
- Use time and location codes that insiders understand
- Provide alternative contact methods

Creating Effective Physical Materials

Design principles:

- Look professionally made but not expensive
- Use local print shops, pay cash
- Include multiple ways to get involved
- Focus on community benefit, not political ideology
- Make information actionable and specific

Content guidelines:

- Lead with community concerns (housing, safety, education)
- Offer practical solutions and mutual aid
- Provide clear next steps for engagement
- Include success stories from similar communities
- · Avoid inflammatory language or obvious political messaging

CHAPTER 5: CASH-BASED MUTUAL AID SYSTEMS

Why Cash-Based Systems Matter

Digital payment systems create detailed transaction records that can be analyzed for patterns. Cash transactions are anonymous and can't be tracked or reversed by authorities.

Setting Up Cash-Based Mutual Aid

Step 1: Identify Community Needs

- Food assistance
- Rent and utility support
- Transportation costs
- Medical expenses
- Child care assistance
- Emergency funds

Step 2: Create Collection Systems

- Weekly community meals with voluntary contributions
- Service exchanges (skills for donations)
- Community yard sales and markets
- Fundraising events (concerts, art shows)
- Anonymous donation boxes in community spaces

Step 3: Establish Distribution Protocols

- Regular distribution days/times
- Anonymous request systems

- Trusted community member verification
- Emergency rapid-response systems

Cash Security and Management

Security protocols:

- Never store large amounts in single location
- Use multiple trusted holders
- Maintain simple paper records only
- · Count money with witnesses present
- Transport funds in small amounts

Record keeping:

- Track only amounts and general categories
- Never record names or specific situations
- Use codes for different types of assistance
- Store records separately from funds
- Review and dispose of records regularly

Building Trust Without Documentation

Reputation systems:

- Personal recommendations from trusted community members
- Demonstrated commitment through volunteer work
- Participation in community activities over time
- Accountability through social connections

Verification methods:

• In-person interviews for ongoing assistance

- Community member vouching system
- Trial periods for new participants
- Regular check-ins with recipients

CHAPTER 6: COUNTER-SURVEILLANCE FOR ORGANIZERS

Understanding How You're Being Watched

Digital surveillance:

- Phone location tracking
- · Social media monitoring
- Email and message interception
- Financial transaction monitoring
- Facial recognition systems

Physical surveillance:

- Direct observation by human agents
- Vehicle tracking devices
- Photography/video recording
- Infiltration by informants

Detecting Surveillance

Signs of digital surveillance:

- Unusual battery drain on devices
- Slow internet or phone performance

- Receiving targeted ads related to private conversations
- Friends mentioning they received ads after spending time with you

Signs of physical surveillance:

- Same vehicles or people appearing in multiple locations
- People who seem out of place in community settings
- Questions about your activities from casual acquaintances
- New community members who ask lots of questions but don't participate

Counter-Surveillance Techniques

Digital counter-surveillance:

- Leave phones at home during sensitive activities
- Use burner phones with cash-purchased service
- Communicate important information only in person
- Create false digital trails to confuse tracking systems
- Use public computers for any necessary online activity

Physical counter-surveillance:

- Vary your routes and schedules
- Meet in locations with multiple exits
- Use counter-surveillance walks before important meetings
- Conduct sensitive discussions while walking or in loud environments
- Build relationships slowly and verify through multiple interactions

Operational Security (OPSEC) for Organizers

Information compartmentalization:

Share information only with people who need to know

- Use different people for different aspects of operations
- Never discuss one group's activities with another group
- Keep written records minimal and coded

Communication security:

- Important discussions happen only face-to-face
- Use coded language even in person
- Establish secure meeting protocols
- Create backup communication methods

Personal security:

- Don't organize alone always work with trusted partners
- Inform trusted people of your schedule and expected return times
- Establish check-in protocols for potentially risky activities
- Prepare family and friends for possible harassment or legal issues

CHAPTER 7: EMERGENCY COMMUNICATION PROTOCOLS

When Digital Networks Fail

Emergency situations often involve communication disruptions, either accidental (disasters) or intentional (government shutdown of networks). Analog communication systems become critical during these periods.

Emergency Communication Hierarchy

Priority 1: Life Safety

• Medical emergencies

- Immediate physical threats
- Natural disasters
- Essential resource needs (water, shelter, medication)

Priority 2: Security Alerts

- Law enforcement raids
- Infiltration warnings
- Surveillance escalation
- Community member arrests or disappearances

Priority 3: Coordination

- Resource distribution
- Meeting changes
- Information sharing
- Network status updates

Emergency Ham Radio Procedures

Activation protocols:

- Designated emergency frequencies
- Specific times for emergency nets
- Authentication codes for operators
- Chain of command for information relay

Message handling:

- Emergency traffic takes precedence over all other communication
- Messages numbered and time-stamped
- Confirmation required for critical information

Backup operators designated for each primary

Sample emergency net script: "This is [CALL SIGN] activating emergency net on [FREQUENCY]. All non-emergency traffic please clear frequency. Emergency stations check in now."

Physical Emergency Signals

Community alert systems:

- Predetermined signals visible from multiple locations
- Color-coded alert levels
- Time-based signal variations
- Backup signal methods

Examples:

- Colored cloth or flags in specific locations
- Light patterns in windows
- Chalk marks on designated surfaces
- Arrangements of common objects

Emergency Supply Protocols

Communication supplies:

- Battery-powered radios (multiple types)
- Backup batteries and charging systems
- Spare equipment stored in multiple locations
- Emergency frequency lists and protocols

Information supplies:

- Contact lists (memorized or hidden)
- Code books and reference materials

- Maps of local area and evacuation routes
- Cash reserves for emergency needs

CHAPTER 8: THE "FEED THE BIRDS" CODE SYSTEM

Origin and Philosophy

"Feed the birds" originated as a recognition phrase between resistance network members. The phrase draws on the idea that information, like bird seed, should be spread widely to nourish the community.

Basic Code Structure

Recognition phrases:

- Challenge: "Do you know where I can get birdseed around here?"
- **Response:** "The best place is to ask the neighbors they feed them every day."
- Counter-challenge: "What kind of birds do you usually see?"
- Final response: "The kind that sing in the morning."

Information Classification

Seed types (information categories):

- **Sunflower seeds:** General community information
- Millet: Meeting times and locations
- Safflower: Security alerts and warnings
- **Thistle:** Financial/resource information
- Mixed seed: Complex information requiring multiple sources

Bird types (urgency levels):

• **Sparrows:** Routine information

• Cardinals: Important but not urgent

• Blue jays: Urgent attention required

• Hawks: Immediate action required

• **Owls:** Night/emergency protocols

Conversation Integration

The code system works by integrating coded information into normal conversations about bird feeding and watching.

Example conversation:

- Person A: "I noticed the cardinals have been active lately."
- Person B: "Yes, I think they're looking for safflower seeds."
- **Translation:** Important security alert requiring attention.

Extended example:

- Person A: "The blue jays seem really agitated this morning."
- Person B: "I heard they found some fresh thistle seed behind the community center."
- Person A: "That's good I know some sparrows who would be interested."
- **Translation:** Urgent financial information available at dead drop location, suitable for distribution to general network.

Advanced Code Techniques

Temporal coding:

- "Morning birds" = immediate timeframe
- "Evening birds" = delayed timeframe

- "Migrating birds" = temporary situation
- "Nesting birds" = long-term/permanent situation

Location coding:

- "Backyard" = safe/secure location
- "Park" = public meeting space
- "Feeder" = information source
- "Birdhouse" = safe house or secure facility
- "Migration route" = communication pathway

Security Protocols

Code security:

- Never write down code meanings
- Teach codes only through direct personal contact
- Change codes periodically or when compromise is suspected
- Use codes only with verified network members
- Have backup code systems ready

Natural integration:

- Study local bird species to make conversations authentic
- Actually participate in bird watching activities for cover
- Learn enough about bird feeding to sustain extended conversations
- Use real local bird information to support coded communications

CHAPTER 9: BUILDING ANALOG COMMUNITY NETWORKS

Network Structure Principles

Cell structure:

- Small groups of 3-5 trusted individuals
- Each cell operates independently
- Limited knowledge of other cells
- Single liaison person connects to other cells
- Geographic or functional organization

Hub system:

- Central coordination points for resources and information
- Multiple backup hubs in different locations
- Rotating leadership to prevent single points of failure
- Clear protocols for hub-to-hub communication

Recruitment and Vetting

Organic recruitment:

- Start with existing relationships
- Build through community service activities
- Recruit people who demonstrate commitment over time
- Use multiple references and verification methods

Vetting process:

- Initial recruitment through trusted connections
- Period of observation in community activities

- Gradual increase in responsibilities and information access
- Regular evaluation of reliability and security practices

Red flags:

- New community members who ask many questions
- People who push for faster advancement or more information
- Anyone who suggests illegal activities or violence
- Individuals with unexplained resources or background gaps

Skills and Resource Sharing

Essential skills for analog networks:

- Ham radio operation and maintenance
- Basic first aid and medical training
- Gardening and food preservation
- Mechanical and repair skills
- Financial management and accounting
- Teaching and education abilities
- Legal knowledge and advocacy

Resource sharing systems:

- Tool libraries and equipment sharing
- Skill exchange networks
- Emergency supply coordination
- Transportation and logistics support
- Safe house networks for temporary shelter

Meeting Security and Protocols

Meeting locations:

- Public spaces with multiple exits
- Locations with legitimate reasons for gatherings
- Rotating meeting places and times
- · Backup locations for every planned meeting
- Counter-surveillance protocols for sensitive meetings

Meeting procedures:

- Arrive and leave separately
- Limit meeting duration
- No phones or recording devices
- Written notes taken only when necessary and destroyed after use
- Clear agenda and time limits for discussions

CHAPTER 10: LEGAL CONSIDERATIONS AND SAFETY PROTOCOLS

Know Your Rights

First Amendment protections:

- Freedom of speech and assembly
- Right to distribute literature in public spaces
- Protection for peaceful protest and demonstration
- Right to associate with others for legal purposes

Fourth Amendment protections:

- Protection against unreasonable searches
- Warrant requirements for searching private property
- Right to refuse consent for searches
- Protection for private communications

Legal limitations:

- Incitement to violence is not protected speech
- Some public spaces have restrictions on assembly or literature
- Private property rights limit access and activities
- Laws vary by state and locality

Interacting with Law Enforcement

If stopped or questioned:

- Remain calm and polite
- Ask if you're free to leave
- If detained, ask for a lawyer
- Don't answer questions without legal representation
- Don't consent to searches

If your home is searched:

- Ask to see the warrant
- Don't interfere with the search
- Take notes on what's searched and taken
- Contact a lawyer immediately
- Don't answer questions without legal representation

Protecting Yourself and Your Network

Personal security:

- · Keep minimal records and information at home
- Use secure communication methods for sensitive information
- Inform trusted people of your activities and schedule
- · Have legal representation identified before you need it
- Keep emergency funds available for bail and legal costs

Network security:

- Compartmentalize information and activities
- Use multiple communication methods with backup plans
- Regularly review and update security protocols
- Plan for compromise scenarios
- Train all members in legal rights and proper responses

Emergency Legal Protocols

If someone is arrested:

- Don't discuss the situation over phones or digital communications
- Contact predetermined legal support immediately
- Organize bail funds and legal fee support
- Provide support for family members
- Review network security to prevent further compromises

Legal support resources:

- Identify lawyers who handle civil rights cases
- Know local bail bond procedures and costs

- Maintain emergency legal fund for network members
- Create legal observer training for demonstrations
- Establish relationships with legal aid organizations

Avoiding Illegal Activity

Focus on legal organizing:

- Community service and mutual aid
- Voter registration and education
- Legal protest and demonstration
- · Information sharing and education
- Supporting legal political candidates and causes

Avoid illegal activities:

- Vandalism or property destruction
- Trespassing on private property
- Threats or intimidation
- Any form of violence
- Truly illegal surveillance or intelligence gathering

CONCLUSION: BUILDING RESILIENT COMMUNITIES

The techniques in this toolkit aren't just about avoiding surveillance - they're about building stronger, more resilient communities that can support each other through difficult times.

Digital tools have made us dependent on centralized systems that can be monitored, controlled, or shut down. Analog organizing creates independent community infrastructure that can't be easily disrupted by outside forces.

Getting Started

Week 1: Choose one technique from this toolkit to implement

Week 2: Find two other people interested in community resilience

Week 3: Attend a local community meeting or volunteer activity

Week 4: Set up basic emergency communication capability

Week 5: Start building relationships with neighbors

Week 6: Identify local resources and mutual aid opportunities

Remember

- Strong communities don't need digital coordination
- Trust is built through consistent action over time
- Small, local networks are more secure than large, distant ones
- The goal is community resilience, not resistance for its own sake
- Legal, ethical organizing is more sustainable than underground activity

Final Words

Every authoritarian system in history has been defeated by ordinary people who cared more about their communities than their own safety. The tools in this guide give you ways to organize that can't be easily tracked, predicted, or suppressed.

Use them wisely. Share them carefully. Build something worth defending.

Feed the birds.

The Underground Archive

"Still here, still documenting, still resisting"

For more resources and ongoing intelligence, join our secure newsletter at https://www.americanautocracy.org

APPENDIX: QUICK REFERENCE GUIDES

Ham Radio Quick Start

- 1. Get licensed (study online, take test locally)
- 2. Buy basic handheld radio (\$25-50)
- 3. Program local frequencies
- 4. Practice with local clubs
- 5. Establish regular check-in schedule

Dead Drop Checklist

- [] Location selected with multiple access routes
- [] Signal system established
- [] Timing protocol agreed upon
- [] Waterproof containers prepared
- [] Information coding system ready

Emergency Communication Plan

- [] Ham radio equipment and backup batteries
- [] Emergency frequency list memorized
- [] Physical signal system established

- [] Network check-in procedures practiced
- [] Legal support contacts identified

"Feed the Birds" Quick Reference

- Recognition: "Do you know where I can get birdseed?"
- **Response:** "Ask the neighbors they feed them daily"
- Urgency levels: Sparrows (routine) → Cardinals (important) → Blue jays (urgent) → Hawks (immediate)
- **Information types:** Sunflower (general) → Millet (meetings) → Safflower (security) → Thistle (resources)

Legal Rights Summary

- **First Amendment:** Free speech, assembly, petition
- **Fourth Amendment:** Protection from unreasonable search
- When stopped: Ask if free to leave, request lawyer
- If arrested: Stay silent, request lawyer, don't consent to searches

Important Notice

The American Autocracy Universe is a work of fiction created for educational and entertainment purposes. All organizations, characters, policies, and events described are entirely fictional and do not represent any real government agency, political organization, or individuals.

Any resemblance to actual government documents, policy proposals, or political strategies is purely coincidental and intended to illustrate historical patterns of authoritarian governance for educational purposes.

This content is protected speech under the First Amendment and is not intended to promote, encourage, or provide instruction for any illegal activities.

About the Creator

Greg Wolford is the creator of The American Autocracy Universe. This multimedia storytelling project spans blogs, podcasts, newsletters, and fiction to explore themes of resistance, documentation, and hope in the face of systematic oppression.

© 2025 Greg Wolford. Truth survives.

"Democracy dies in darkness. But it also dies in plain sight, when people stop paying attention."