The Narrow Path

Digital Security, Community Organizing, and Network Coordination for Ordinary Americans

Lisan Kynes

The Narrow Path
Digital Security, Community Organizing, and Network Coordination for Ordinary Americans

First published 2026

Contents

How to Use This Book

Read it in order. Each chapter builds on the one before it. You can't build a secure group without first understanding your own exposure. You can't coordinate across groups without first understanding how a single group holds together.

Level 1: See Clearly (Chapters 1–12) covers individual digital security — what's being collected about you, how to close the most dangerous gaps, and how to recognize when information has been manipulated. This is the foundation.

Level 2: Find Each Other (Chapters 13–26) covers the harder thing: finding people, building trust with them, making decisions together, and surviving the difficult middle stretch where most groups break apart. By the end of this level, you have a functioning team.

Level 3: Build Together (Chapters 27–36) covers connecting groups into something larger — shared governance, joint action, conflict resolution, and reproducing what you've built so others can use it without you.

If you're new to these subjects, this book is written for you. The sequence assumes no prior knowledge.

If you're experienced in operational security or community organizing, Level 3 is probably where this book offers you the most — governance frameworks, coalition structures, and network coordination patterns drawn from documented organizing traditions. The earlier levels may still surface something useful; they're grounded in research, not assumptions about what readers already know.

If you want to introduce someone to these subjects — a friend, a family member, someone who senses that something is wrong but doesn't know where to start — share this book with them.

Level 1

See Clearly

Chapter 1

See Yourself

There's a scene in Dune — the second film — where Paul is able to see the future clearly. Not one future. All of them. Millions of potential paths branching and converging, and almost every one of them ends the same way. The galaxy devolves into holy war. Countless dead. Civilizations collapse. Everything destroyed by forces that are already in motion. But he sees a path, a narrow path, that leads to survival. The Fremen call him the voice from the outer world. They believe he can save them.

I watched that scene in the theater a couple years ago and thought it was beautiful, hopeful, unsettling. Then I went back to my life, which involves getting to the lab by seven, mass producing terrible coffee, and spending my days trying to make sophisticated systems do things they weren't designed to do.

I work in AI research. I evaluate frontier models — the new, experimental stuff. I design tests, probe for capabilities, look for failures, and write reports about what I find. I'm pretty good at it. Most of the time it's tedious, technical, and frustrating. But don't get me wrong, it's incredibly important work, always exciting and I'm grateful to be a part of it.

I have a cool job but it doesn't protect me from feeling what a lot of you feel: that the ground is shifting and the clouds are growing darker. I just want to look forward to the future again. I just want to feel hopeful, relaxed, free.

I didn't do anything about it. I didn't know what to do. I went to work. I ran my evals. I voted. I donated to my favorite organizations. I felt the dread and I carried it the way everyone carries it — by not looking at it directly and hoping people with more power than me were handling it. I can only have so many existential crises in a single week.

Then, things changed. I was assigned an evaluation protocol for a new model. During the session, I deviated from the standard script. I saw something.

The model runs projections. Lots of models do forecasting. What made

this different was the resolution: not trend-level predictions, but the interaction between systems. How a set of specific surveillance capabilities, deployed under a specific legal authority, changes the behavior of a specific population in ways that cascade simultaneously, over time.

It literally runs millions of scenarios. Different starting conditions, different variables, different outcomes.

Most scenarios converge on what I'll just call sub-optimal outcomes. Not a galactic holy war. Just…sub-optimal.

I spent four days trying to break the projections. I stress-tested assumptions. I looked for contamination, confirmation bias, feedback loops that would amplify worst cases. I know how models fail, hallucinate, deviate. I know how really impressive outputs can conceal shallow reasoning.

The projections held. They held because the inputs were real. The surveillance tools were real. The psychometric data was real. The legal frameworks were up-to-date. The model isn't predicting anything exotic. It's working with real data and leading to predictable conclusions.

And then I saw a divergence. A path that bent toward a different outcome. I thought of Paul. I felt, optimistic. Briefly.

In the scenarios where things don't collapse there's a single common denominator. It's not a hero from the outer world. It's not a new technology. It's not an Amendment to the Constitution. It's human beings doing the thing that got us to this point — working together. Small groups. Locally rooted. Autonomous but connected. It was just people with skills, trusting each other, and coordinating to act when it mattered. That was the thread holding things together.

That was my Dune moment. That's when I decided I had to show others the path.

I didn't sleep that night. It wasn't dread that kept me awake. It was an overwhelming sense of clarity. I had a new purpose.

So I did what a researcher does. I started researching.

I started with what I know — artificial intelligence and surveillance technologies. How our data moves through systems that you've probably never heard of. How social movements are monitored, infiltrated, and disrupted, and how some of them survived anyway. How people find each other when trust is scarce. How small groups form, hold together, and learn to work with other small groups without anyone in charge. How networks become resilient, flexible, powerful.

I read the court filings and the congressional records and the declassi-

fied documents. I studied the history. I talked to people who've done this work — organizers, security researchers, people who've built the kind of infrastructure that holds up when institutions don't.

I'm not asking you to believe me. I'm asking you to walk with me. Learn where the path leads. See things for yourself. Everything I share about systems, infrastructure, legal frameworks, and history — check it. Use primary sources. Court filings. Congressional records. Published research. If you do the work with me and the ground gets less solid, walk away. The skills I will teach you work whether or not you think I'm credible. Securing your digital life is smart regardless. Understanding how your data moves through the world is good information regardless. These things make you and the people you care about safer, no matter which direction the future bends.

Finding the narrow path requires that we see things clearly.

Go to your phone. Open your location history.

If you're on iPhone: Settings → Privacy & Security → Location Services → System Services → Significant Locations. It'll ask for your passcode. It should.

If you're on Android: Open Google Maps → tap your profile picture → Your Timeline.

Look at it. See how far back it goes. See how precisely it tracks where you've been, when, for how long. Every place you've slept. Every doctor's office. Every protest, every church, every bar, every yoga class, every person's house you've visited.

Don't delete it yet. Don't change anything yet. Just look. Let it sink in.

Then think about who else has access to this. Your phone carrier. App developers. Data brokers. Law enforcement (often without a warrant). I'll talk more about this in the next chapter.

Summary

You carry a detailed record of everywhere you've been, and it's accessible to more people than you think. Before you can protect yourself, you need to see what you're broadcasting. This chapter is about looking — really looking — at the data trail you leave behind every day.

Action Items

- Check your location history (iPhone: Settings → Privacy & Security → Location Services → System Services → Significant Locations; Android: Google Maps → profile → Your Timeline)
- Review how far back the data goes and how precise it is
- Don't change anything yet — just observe and sit with what you find

Key Terms

- **Frontier model** — The newest, most capable AI systems, typically developed by a small number of labs and evaluated before wider release
- **Evaluation (eval)** — A structured test designed to assess what an AI model can and can't do, including capabilities that could be dangerous
- **Location history** — A detailed log, maintained by your phone's operating system and apps, of everywhere your device has been — often going back years

Chapter 2

The Invisible Auction

You looked.

Good. I know that wasn't easy. Some of you are still sitting with it — every doctor's visit, every late-night drive, every address you thought was private, logged and timestamped and waiting for anyone who asks.

The location history on your phone is the least of it.

When I started researching what ordinary people actually need to understand about surveillance, this is where everything converged. I'm not a surveillance specialist — I'm an evaluation researcher with a unique insight into these systems. I spent two weeks reading court filings, congressional testimony, and investigative reports, and what I found is that the most dangerous pipeline isn't some classified government program. It's a commercial system that runs on your phone right now, and nobody explains how it works.

Here's what happens to your location data after it leaves your phone.

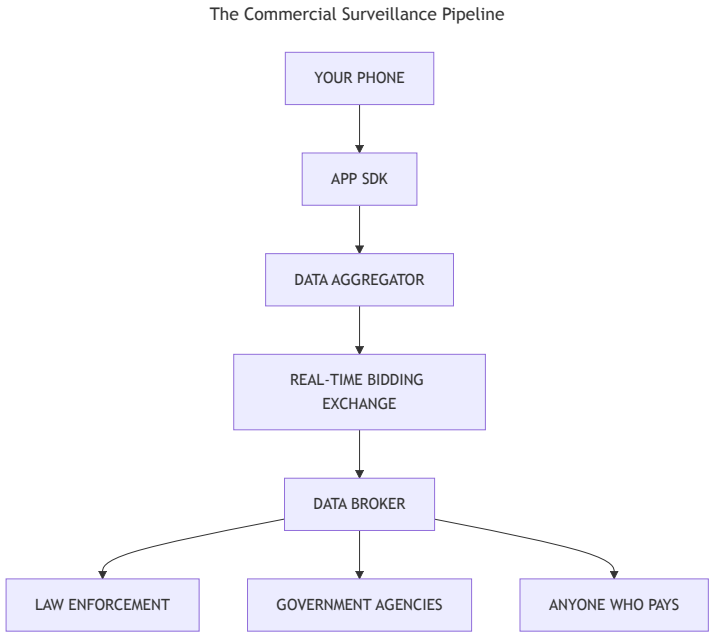
You open a weather app. The app has a piece of code embedded in it — an SDK, a software development kit — put there by a data company you've never heard of. The moment the app checks your location to show you tomorrow's forecast, the SDK copies that location data and sends it somewhere else. Not to the weather company. To a data aggregator.

The aggregator bundles your location with millions of others and feeds it into a real-time bidding exchange — the same system that decides which ads you see. Hundreds of times per day, your phone's location is broadcast to dozens of companies in the time it takes the ad to load. That's not a metaphor. The auction literally happens in milliseconds while you're waiting for a webpage to finish rendering.

From the bidding exchange, your data flows to a data broker. The broker doesn't just have your location from the weather app. It has your location from every app on your phone that runs an SDK — your games, your period tracker, your meditation app, your news reader. It correlates all of it using a single identifier your phone broadcasts to every app you've

installed.

That identifier is called your advertising ID. On Android it's called your MAID. On iOS it's your IDFA. Think of it as a serial number for your entire digital life — and it was on by default when you set up your phone. Every app can read it. Every SDK can copy it. Every data broker can use it to stitch together a pattern of your movements, your habits, your relationships, your health conditions, your beliefs, into a profile attached to a persistent unique number.



Now here's where it stops being abstract.

The data broker sells that profile. Not to advertisers. To anyone who pays. A company called Fog Data Science sold location data to local law enforcement agencies across the country — no warrant, no subpoena, no judicial oversight. The police bought access the way you'd buy a software subscription. A company called Babel Street built a product called Locate X that lets federal investigators track device movements using commercially harvested location data — no warrant required. Contracts show it's been purchased by CBP, ICE, the Secret Service, and the Treasury Department.

I need you to see the shape of this, because it's not what most people think government surveillance looks like. There's no wiretap order. There's no judge. The government doesn't need to surveil you — it just

buys the data that your phone already gave away for free. The pipeline runs from your weather app to a government database, and every link in the chain is technically legal because you clicked "I agree" on a terms of service document that was designed to be unreadable.

This is the single vulnerability you can most effectively address right now. Not because it's the scariest thing out there. It's not. Because it's the one open hole you can partially close in five minutes.

Let's take two more steps, together.

First: delete your advertising ID.

On Android: Settings → Privacy → Ads → Delete advertising ID. Google made this option available in Android 12. If you don't see it, search your settings for "advertising."

On iPhone: Settings → Privacy & Security → Tracking → turn off "Allow Apps to Request to Track." Then go to Settings → Privacy & Security → Apple Advertising → turn off Personalized Ads.

This doesn't make you invisible. Apps can still use other fingerprinting techniques. But it removes the one persistent identifier that makes it trivially easy for brokers to correlate your activity across every app on your phone. You just pulled the thread that held the profile together.

Second: audit your app permissions.

Go to your location permissions. On both platforms it's under Settings → Privacy → Location Services (or Location on Android). Look at every app that has "Always" access to your location. Change it to "While Using App" or "Never" for anything that doesn't need to know where you are in real time. Your weather app does not need "Always." Your shopping app does not need "Always." Your social media app does not need "Always."

Be aggressive. If an app stops working without location access, you can always turn it back on. Most won't even notice.

That's it. That's today's work. Two changes, five minutes, and you've closed the cheapest, most efficient pipeline between your daily life and a government procurement database.

Before the next chapter, I need you to start keeping a record.

If you're going to keep reading, you need somewhere to track what you've done and what you're learning. Not on Google Docs. Not on Notion. Not on anything that stores your data on someone else's server. I'll explain why that matters in detail later. For now, trust the principle: a record of your security posture should be stored the way you'd store any-

thing you want to keep private.

A paper notebook works. If you're more comfortable with software, look at Obsidian or Logseq — both are free, both store everything locally on your device. Nothing leaves your machine unless you choose to sync it.

Start your record with what you've done so far. Checked your location history. Deleted your advertising ID. Audited your app permissions. Write down what you found and what you changed. This is your field journal. It will serve you at every step along the path.

In 2021, a Catholic monsignor — the top administrator of the US Conference of Catholic Bishops — was identified as a user of a dating app by a Catholic publication that purchased commercially available location data. Not hacked. Purchased. They bought app signal data from a broker, correlated the "anonymized" location patterns with the monsignor's known addresses — his office, his home, the conference hotel during a bishops' meeting — and reconstructed his private behavior from commercially available records.

He was forced to resign. He wasn't a spy. He wasn't a criminal. He was a private person whose private life was reconstructed because his phone's advertising ID connected his app usage to his physical locations, and a data broker sold that connection to anyone who wanted it.

I'm not going to name him in this chapter. Look it up. The sources are public — Washington Post, Time, NBC News all covered it. Find the name. Read what happened. Then come back for the next chapter.

This is the first exercise in a skill you're going to need: lateral research. Finding information that's public but not handed to you. Verifying it through multiple sources. Following a thread. You have everything you need.

Summary

Your phone broadcasts a unique identifier — your advertising ID — to every app you use. Data brokers collect this signal, correlate it with your location data, and sell the resulting profile to anyone who pays, including law enforcement agencies operating without warrants. This commercial surveillance pipeline is the single easiest vulnerability to partially close: delete your advertising ID and audit your app permissions.

Action Items

- Delete your advertising ID (Android: Settings → Privacy → Ads → Delete advertising ID; iPhone: Settings → Privacy & Security → Tracking → disable "Allow Apps to Request to Track," then Settings → Privacy & Security → Apple Advertising → disable Personalized Ads)
- Audit app location permissions — change "Always" to "While Using App" or "Never" for every app that doesn't need real-time location
- Set up your field journal: a paper notebook, or a local-first tool like Obsidian or Logseq
- Record what you've done so far (location history check, advertising ID deletion, permission audit) and what you found
- Look up the monsignor case study — find the name through independent lateral research using public sources

Case Studies & Citations

- **Fog Data Science** — Sold location data to local law enforcement agencies without warrants or subpoenas. Reported by the Associated Press and the Electronic Frontier Foundation.
- **Babel Street / Locate X** — Built Locate X, a location surveillance product that tracks device movements using commercially harvested app data. Contracts with CBP, ICE, the Secret Service, and the Treasury Department documented through FOIA requests and reporting by Protocol, The Intercept, and Motherboard/Vice.
- **Venntel** — A subsidiary of the commercial data company Gravy Analytics. Sold location data to ICE and CBP. Investigated by the DHS Inspector General.
- **Defense Department prayer app data** — The U.S. military purchased location data harvested from Muslim prayer apps. Reported by Motherboard/Vice.
- **Monsignor case (2021)** — A senior Catholic official identified through commercially purchased location data correlated with known addresses. Covered by Washington Post, Time, and NBC News. (Name intentionally withheld — finding it is the chapter's lateral research exercise.)

Templates, Tools & Artifacts

- **Field Journal** — Start an offline record of your security actions and findings. Recommended tools: paper notebook, Obsidian (free, local-first), or Logseq (free, local-first). Do not use cloud-based tools like Google Docs or Notion.

Key Terms

- **SDK (Software Development Kit)** — A package of code that app developers embed in their apps, often provided by third-party data companies. The SDK collects data from the app and sends it to the data company — usually without the user's knowledge.
- **Advertising ID (MAID / IDFA)** — A unique identifier assigned to your phone, broadcast to every app you install. Android calls it a MAID (Mobile Advertising ID); Apple calls it an IDFA (Identifier for Advertisers). It's the thread that lets data brokers stitch your activity across apps into a single profile.
- **Data broker** — A company that collects, aggregates, and sells personal data — including location data — to commercial and government buyers.
- **Real-time bidding (RTB)** — The automated auction system that decides which ads you see. Your phone's location and other data are broadcast to dozens of companies in milliseconds during each auction. The same system that serves ads also feeds the data broker pipeline.

Chapter 3

What Are You Actually Protecting?

You've seen your location history — every place you've been, timestamped, waiting. You've seen the pipeline — how your weather app feeds data through an auction system to brokers who sell it to anyone who pays, including law enforcement agencies that never bothered with a warrant. You deleted your advertising ID. You audited your app permissions. If you did the research exercise, you found the name I didn't give you, and you understand now that commercially available data can reconstruct anyone's private life from the patterns their phone leaves behind.

There's a scene in Ender's Game — the book, not the movie — where Ender enters the Battle Room for the first time. Zero gravity. No map. No briefing on the enemy's position. Most of the kids start flailing, trying to orient themselves to the room as if there's still an up and a down. Ender's instinct is different. He reorients. He picks a direction and decides: the enemy's gate is down. He defines the terrain relative to his objective, not relative to what's comfortable.

That's what I need you to do now. Focus on the objective.

Everything I've shown you so far has the same problem: it's general. The surveillance pipeline affects everyone. The advertising ID was on every phone. The data brokers sell everyone's data. That's true, and it's also the reason most people hear about this stuff and do nothing — because "everyone is affected" feels the same as "no one can do anything." It's paralyzing.

The way through paralysis is specificity. Not "surveillance is bad" — that's abstract. Instead: what am I actually protecting, and from whom?

Those questions have an answer. It's called a threat model.

It's not a fancy term. It's not paranoia. It's the exercise of sitting down and mapping your specific situation — your risks, your adversaries, your vulnerabilities — before a crisis forces you to figure it out under pressure. Security professionals do this. Journalists do this. Lawyers do this for their clients. I write them at work — they're boring documents, spreadsheets

mostly. Risk on one axis, likelihood on the other, mitigation steps in the third column.

The fact that ordinary people don't do this isn't because it's hard. It's because no one ever told them it was valuable.

I spent time with the EFF's Surveillance Self-Defense project — the Electronic Frontier Foundation, a nonprofit that's been defending digital rights since 1990. They developed a framework that boils threat modeling down to five questions. I'm going to give them to you, and then I'm going to show you why they matter with a story about an innocent man who just wanted to ride his bike.

Five questions. Write them in your field journal. Answer honestly.

One: What do I have that's worth protecting?

Not just "my data" — be specific. Your location patterns. Your communications with specific people. Your browsing history. Your medical records. Your financial information. Your political activity. Your relationships. Think about which pieces of your life, if exposed to the wrong person, would cause real harm.

Two: Who might want access to it?

This is where most people's thinking stops too early. You might think "hackers" or "the government" and leave it there. Be more specific. An abusive ex-partner. An employer who monitors social media. A data broker selling to anyone who pays. A law enforcement agency using a geofence warrant. A neighbor with a grudge and a people-search website. Your threats are specific to your life. Name them.

Three: How likely is it that I'd need to protect it?

Some threats are theoretical. Some are already happening. If you're a teacher and a parent has already emailed you threats, that's not hypothetical — that's a present threat and it changes your entire calculation. If you're someone who occasionally attends protests, the likelihood that your location data matters to law enforcement is not zero, but it's different from the likelihood facing a full-time organizer. Be honest about where you actually are, not where you might be someday.

Four: How bad would it be if I failed?

This is the question that makes the whole exercise real. For some threats, the consequence of failure is an awkward conversation. For others, it's job loss. For others, it's physical danger. A data breach that exposes your email password is annoying. A data breach that exposes your home address to someone who's threatened you is life-threatening. The severity determines

how much effort the protection is worth.

Five: How much trouble am I willing to go through to prevent it?

Security always has a cost — in time, in money, in inconvenience. The perfect security posture is the one you'll actually maintain. If a recommendation is too burdensome to follow consistently, it's worse than a simpler one you'll stick with. This question keeps you honest. You're building something sustainable, not performing security theater for a week before going back to your old habits.

Here's why this matters in practice.

In March 2019, a man named Zachary McCoy went for a bike ride in his neighborhood in Gainesville, Florida. He used an app called RunKeeper to track his mileage — the same kind of fitness tracking millions of people do without thinking about it. His route happened to loop past a house that was burglarized that same day.

Ten months later, he got an email from Google. Local police had served a geofence warrant — a request that told Google to hand over information on every device that was near a specific location during a specific time window. McCoy's phone, broadcasting his location to Google through his fitness app, had been in the area. He was now a suspect in a burglary he knew nothing about.

He had seven days to go to court or Google would release his account information to police.

McCoy wasn't a criminal. He wasn't an activist. He wasn't a person anyone would describe as "high risk." He was a guy who rode his bike and used an app to count the miles. He had to go to his parents, explain what was happening, and they dipped into their savings to hire a lawyer. The lawyer challenged the warrant. The police eventually withdrew it — but McCoy spent thousands of dollars and months of anxiety proving that his bike ride was a bike ride.

Here's the thing: if McCoy had sat down before any of this happened and answered those five questions, his assessment would have been reasonable and low-key. I'm not a public figure. I'm not an activist. My main digital risk is the usual stuff — breaches, spam, maybe identity theft. And his conclusion — I don't need to go to extreme lengths — would have been perfectly rational.

But he also would have known that his fitness app was sharing location data with Google. He would have understood that location data could be

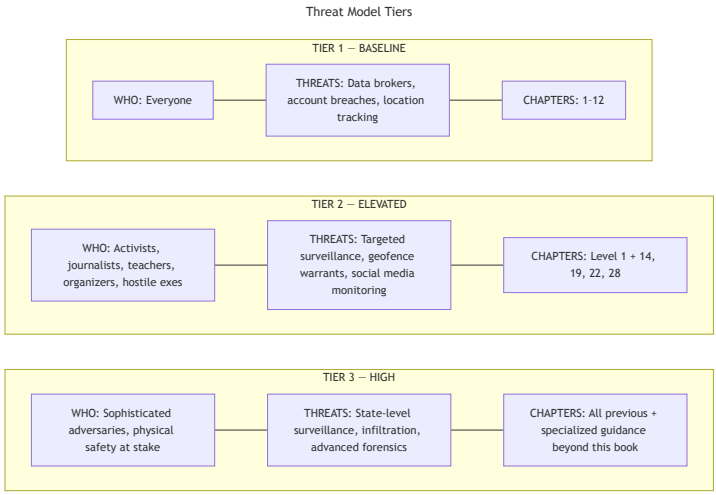
swept up in warrants he'd never know about. And he might have turned off location sharing for that one app, or used one that stores data locally, or simply understood the risk he was accepting. Not because he was paranoid. Because he'd thought about it.

That's the difference a threat model makes. It doesn't tell you to lock everything down. It tells you what you're choosing to leave open, and makes that choice conscious instead of invisible.

Most people, working through these five questions honestly, will land somewhere I'd call Tier 1, the lowest level. Tier 1 means you face the baseline risks that come from existing in a surveillance economy. Data brokers have your information. Your accounts have probably been breached. Your location history exists somewhere. The steps you've already taken — deleting your advertising ID, auditing app permissions — are Tier 1 responses. The steps coming in the next chapters — password security, encrypted communications — are also Tier 1. They're the foundation everyone should have regardless of their situation.

Some of you will recognize that your situation puts you in Tier 2. You attend protests. You work with vulnerable populations. You're a journalist, or an organizer, or a teacher in a school district where parents have made threats. You have an ex-partner who's shown they'll cross boundaries to find information about you. Tier 2 means the baseline isn't enough — you need additional measures tailored to your specific risks, and we'll get to those.

A few of you will know you're in Tier 3. You know who you are. Your threat model includes sophisticated adversaries or situations where operational security is the difference between safety and physical harm. Later chapters address this, and I'll be honest about where my expertise ends and where you need specialized guidance.



For now, the work is the same regardless of your tier.

Spend fifteen minutes. Open your field journal. Answer the five questions. Be specific and honest. It's not a test. It's a training exercise.

When you're done, you'll have something most people never bother to create: a clear picture of what you're protecting, from whom, and why. Every recommendation I make in the chapters that follow connects back to this framework. When I say "this matters more if you're Tier 2," you'll know whether that's you. When I say "this is probably overkill unless you're Tier 3," you'll know whether to skip it or pay attention.

The threat model is the foundation. Everything else builds on it.

No matter what you wrote down, there's one thing that protects you at every level. It's simple but most people still haven't done it.

Come back when you've completed your threat model. We'll fix it.

Summary

Surveillance affects everyone, but your risks are specific to your life. A threat model is the exercise of identifying what you're protecting, from whom, and how much effort the protection is worth. The EFF's five-question framework turns abstract anxiety into a concrete, personal assessment — and every security recommendation in the chapters ahead connects back to it.

Action Items

- Answer the five threat-modeling questions in your field journal: (1) What do I have worth protecting? (2) Who might want access? (3) How likely is it? (4) How bad would it be? (5) How much trouble am I willing to go through?
- Be specific — name actual data, actual people, actual scenarios rather than generalities
- Identify your tier (1, 2, or 3) based on your honest assessment
- Record your threat model in your field journal — this is the framework every future chapter builds on

Case Studies & Citations

- **Zachary McCoy (Gainesville, FL, 2019–2020)** — Cyclist identified as a burglary suspect after a geofence warrant swept up his fitness app location data. Spent thousands in legal fees to prove his innocence. Never charged. Reported by NBC News and the New York Times.
- **EFF Surveillance Self-Defense** — The Electronic Frontier Foundation's open-access guide to personal digital security, including the five-question threat modeling framework used in this chapter. Available at ssd.eff.org.

Key Terms

- **Threat model** — A structured assessment of what you're protecting, who might want access to it, how likely the threat is, how severe the consequences would be, and how much effort you're willing to invest in protection. The foundation for all personal security decisions.
- **Geofence warrant** — A legal request that compels a technology company (typically Google) to hand over information on every device that was near a specific location during a specific time window — sweeping up everyone in the area, not just suspects.
- **Tier 1 / Tier 2 / Tier 3** — A rough classification of personal risk levels. Tier 1: baseline risks from living in a surveillance economy. Tier 2: elevated risks from activism, journalism, teaching, or personal situations involving hostile actors. Tier 3: risks involving sophisticated adversaries where operational security is a safety issue.

Chapter 4

Your Passwords Are Already For Sale

The simple fix I alluded to in the last chapter has to do with passwords.

I told you it was simple. It is. And I need to show you why it matters before you dismiss it as something you already know about.

Go to haveibeenpwned.com. It's a free service run by a security researcher named Troy Hunt — it aggregates publicly known data breaches and lets you check whether your email address appears in any of them. Type in your primary email. The one you use for everything.

I'll wait.

If you're like most people, you just found out that your email address has been exposed in multiple breaches. The site currently indexes over fifteen billion compromised accounts across more than nine hundred breached websites. Yours are in there. Not because you did anything wrong — because the services you trusted with your data got hacked, and the data ended up in databases that anyone can search.

Now here's the part that turns this from an abstract privacy problem into a concrete security emergency: if you reused the same password across multiple sites — and most people do — then every breach that exposed that password gave an attacker the key to every other account that uses it. This isn't theoretical. It's the single most common way accounts get compromised. An attacker doesn't hack your email — they find the password you used on a shopping site that got breached in 2019, try it on your email, and it works. It has a name: credential stuffing. It's automated, it runs at scale, and it works because human beings are predictable about passwords.

Your email account is the skeleton key to everything else in your digital life. Think about it. When you forget a password to any other service, where does the reset link go? Your email. If someone controls your email, they can reset the password on your bank, your social media, your health portal, your cloud storage — anything tied to that address. Securing your email is not the most interesting security topic. It's the highest-impact single action most people can take.

Two things to do. Both tonight.

First: install a password manager.

I recommend Bitwarden. It's free. It's open-source, which means its code is publicly available and independently audited — you don't have to trust the company's promises about security because anyone can inspect the system. It generates long, random, unique passwords for every account and stores them encrypted. You remember one password — your master password — and Bitwarden handles the rest. 1Password is not open-source but is an excellent alternative and works the same way.

Your master password should be long. Not complex — long. "correct horse battery staple" is stronger than "P@$$w0rd!" and infinitely easier to remember. A passphrase of four or five random common words, maybe with a number thrown in, gives you something that's both memorable and effectively unguessable through brute force. Write it down on paper and keep it somewhere physically secure until you've memorized it. Not in a file on your computer. Paper.

Install Bitwarden or 1Password on your phone and your primary web browser. Perform a password reset for your primary email account — let Bitwarden create it, long and random. Log in with the new password. Save it in Bitwarden. That's one account down.

You're going to be doing this gradually for every account you currently have and every new account you create. Don't try to do them all tonight — you'll burn out and quit. Start with your email. Over the coming days and weeks, every time you log into a site, take thirty seconds to change the password to something Bitwarden generates. The slow migration works. The all-at-once approach doesn't.

Second: turn on two-factor authentication for your email.

Two-factor authentication — 2FA — means that even if someone has your password, they still can't get in without a second piece of proof. Your email provider almost certainly supports it.

Here's the hierarchy, plainly:

SMS-based 2FA — a code texted to your phone — is better than nothing. But it can be defeated by SIM-swapping, where an attacker convinces your phone carrier to transfer your number to their device. This isn't exotic — it happens regularly, and phone carriers have gotten only marginally better at preventing it.

An authenticator app is significantly stronger. Download one — Google Authenticator, Authy, or the one built into Bitwarden itself. It generates a

code that changes every thirty seconds and exists only on your device. No phone number to steal, no text message to intercept.

A hardware security key — a physical USB device like a YubiKey — is the strongest option. It's a small investment and it's overkill for most people's threat models right now. If you wrote "Tier 2" or "Tier 3" in your field journal this morning, look into it. Everyone else: the authenticator app is where you want to be.

Go to your email account's security settings. Enable 2FA. Choose the authenticator app option if it's available. Walk through the setup. It takes three minutes.

Record this in your field journal. Which breaches showed up on HaveIBeenPwned. Your primary email's 2FA status — what method you chose. Which accounts still use reused passwords — you don't need to fix them all now, but write the list. You'll work through it.

Password reuse creates a single point of failure that collapses the boundaries between different parts of your life. Over a thousand people were identified after January 6 through a convergence of digital evidence. But compromised accounts and shared passwords contributed to identification chains most people wouldn't expect. Private messages accessed through breached credentials. Accounts linked through reused passwords. The forensic process of unraveling someone's digital identity is a lot easier when every door opens with the same key.

Whatever's in your threat model — your employer, your ex, a data broker, law enforcement — reused passwords make you an easy target. Unique passwords make the pieces harder to connect.

Your email is now behind a unique password and a second factor. That's the most important account in your digital life, and you just secured it.

But the messages inside that email — and every message you send through every app on your phone — are still readable by anyone who sits between you and the person you're talking to. Your phone carrier. The app company. Anyone with access to the server. Tomorrow I'll show you what "encrypted" actually means, why most of what you think is private isn't, and what to do about it.

Summary

Password reuse is the single most common way accounts get compromised, and your email is the skeleton key to your entire digital life — it's where every password reset goes. Two steps close this gap tonight: a password manager that generates unique passwords for every account, and two-factor authentication that adds a second layer even if a password is stolen.

Action Items

- Check haveibeenpwned.com with your primary email address — see which breaches you appear in
- Install Bitwarden (free, open-source, audited) on your phone and primary browser
- Generate a new unique password for your email account using Bitwarden and log in with it
- Create a strong master password: a passphrase of 4–5 random words, written on paper until memorized
- Enable two-factor authentication on your email — use an authenticator app (Google Authenticator, Authy, or Bitwarden's built-in) over SMS
- Record in your field journal: which breaches appeared, your email's new 2FA status, and a list of accounts still using reused passwords
- Begin the slow migration: every time you log into a site, take 30 seconds to change the password to one Bitwarden generates

Case Studies & Citations

- **HaveIBeenPwned** — Free breach-notification service created by security researcher Troy Hunt. Indexes over 15 billion compromised accounts across 900+ breached websites. Available at haveibeenpwned.com.
- **Credential stuffing** — An automated attack where breached username/password pairs are tested against other services. Effective because most people reuse passwords across sites.
- **SIM-swapping** — An attack where an adversary convinces a phone carrier to transfer a victim's phone number to a new device, intercepting SMS-based two-factor codes. Documented in cases reported by the FBI and FTC.
- **January 6 digital forensics (2021)** — Over 1,000 individuals identified through converging digital evidence including compromised accounts and password-linked identity chains. Social media was the primary vector (covered in the next chapter), but credential reuse contributed to identification pathways.

Templates, Tools & Artifacts

- **Bitwarden** — Free, open-source password manager. Code is publicly available and independently audited. Available at bitwarden.com.
- **Authenticator apps** — Google Authenticator, Authy, or Bitwarden's built-in authenticator. Generate time-based one-time codes that change every 30 seconds.
- **YubiKey** — Hardware security key (USB device). Strongest 2FA option. Recommended for Tier 2–3 threat models.

Key Terms

- **Credential stuffing** — An automated attack that uses stolen username/password combinations from one breach to try logging into other services. Works at scale because most people reuse passwords.

- **Two-factor authentication (2FA)** — A security method requiring two separate forms of proof to access an account — typically a password plus a code from an app or device. Hierarchy: SMS (weakest) → authenticator app (strong) → hardware key (strongest).
- **SIM-swapping** — An attack where someone convinces your phone carrier to transfer your number to their device, allowing them to intercept SMS verification codes.
- **Password manager** — Software that generates, stores, and autofills unique passwords for every account, encrypted behind a single master password.
- **Master password / passphrase** — The single password you memorize to unlock your password manager. A passphrase (multiple random words) is both stronger and easier to remember than a complex short password.

Chapter 5

Who's Listening?

Let me tell you what "encrypted" actually means, because the word gets used so loosely that it's almost stopped meaning anything.

When you send a regular text message — an SMS — it travels from your phone to your carrier's servers to the recipient's carrier's servers to their phone. At every point along that chain, the message is readable. Your phone carrier can see it. Anyone with access to the carrier's infrastructure can see it. Law enforcement can request it with a court order, and carriers comply routinely. The message is transmitted, but it's not protected. Think of it as a postcard — the postal service can read it at every stop along the way.

End-to-end encryption means the message is locked when it leaves your device and only unlocked when it arrives at the recipient's device. Not at the server. Not at the company. Not at any intermediate point. The company running the app literally cannot read your message because they don't have the key. If law enforcement serves them with a subpoena demanding your message content, the company can't hand over what it doesn't have.

That's not a privacy preference. That's an engineering decision with legal consequences. And the difference between apps that make this decision and apps that don't is the difference between your communications being accessible to anyone with a court order — or in many cases, without one — and your communications being accessible only to you and the person you're talking to.

Three apps. I'll be direct about what each one does and doesn't do.

Signal. This is the standard. It's free, it's a nonprofit, and its code is open-source — meaning anyone can inspect exactly how it works. Signal was built from the ground up to collect as little data as possible. When the US government has served Signal with subpoenas — and this has happened multiple times, the cases are public — Signal has produced exactly two data points: the date the account was created and the date it last con-

nected to the service. That's it. Not because they refused to cooperate. Because that's all they have.

No message content. No contact lists. No group memberships. No profile information. No call records. The company publishes every government request they've received alongside their responses at signal.org/bigbrother. It makes for very short reading.

WhatsApp. This is where it gets complicated, because WhatsApp uses Signal's encryption protocol for message content. Your messages are end-to-end encrypted. Meta, WhatsApp's parent company, cannot read them. That part is real.

But Meta collects and retains everything around the messages. Who you talk to. When. How often. From which IP address — which reveals your location. Your phone number, your contacts, your group memberships, your profile photo, your about status. This is metadata, and metadata reveals more than most people realize. If someone knows you called a suicide hotline at 2am, they don't need to know what you said. If someone knows an organizer messaged forty people the night before a protest, they don't need to read the messages to understand what's happening.

Meta complied with roughly 77% of US government data requests in the most recent reporting period. That compliance involves metadata — and metadata is what ties your communications to your identity, your location, your relationships, and your patterns.

iMessage. Apple's messaging is encrypted between Apple devices — the blue bubbles. But when you text someone on Android, iMessage falls back to SMS or RCS, and depending on the configuration, that traffic may not be end-to-end encrypted. If you're in an all-Apple household, iMessage is reasonable for most threat models. If you're not — and you often don't know whether the person on the other end has the same setup you do — you can't count on it.

Apple also stores iCloud backups by default, which can include your message history. If your iCloud backup isn't using Advanced Data Protection — and most people haven't turned that on — Apple can access your backed-up messages when served with a warrant. The encryption exists between devices but may not extend to the copy sitting on Apple's servers.

The distinction I need you to hold onto isn't about any one app. It's about the difference between content and metadata.

Content is what you said. Metadata is everything else — who you

talked to, when, how long, from where, how often. The US government's position, established in practice and upheld by its intelligence agencies for decades, is that metadata collection is less invasive than content collection and therefore subject to weaker legal protections. This is the position that allowed the NSA's bulk phone records collection program that Edward Snowden revealed in 2013.

But General Michael Hayden, who led both the NSA and the CIA, said this publicly: "We kill people based on metadata."

He wasn't being provocative. He was describing how intelligence operations work. Metadata patterns — communication networks, location data, contact frequency — are what targeting decisions are built on. The content of a message is useful for prosecution. The metadata is useful for identification.

This matters for your threat model. If your concern is the content of specific messages, end-to-end encryption addresses it — even WhatsApp works for that. If your concern is that the pattern of your communications reveals information about you — who you know, what you're involved in, how you're organized — then the metadata question is what matters. And for metadata, Signal is the only mainstream option that collects effectively nothing.

Four things. All today.

Install Signal. It's free, available on both platforms, takes two minutes.

Move one important conversation there. Not everything — one. A family group chat. A close friend. A partner. The people whose communications matter most to you. This is the hardest part, because it requires someone else to install it too. I know. Start with one person and work outward.

If people push back — and some will — here's what works: don't lead with surveillance or privacy. Lead with "it's a better app." The group chats are cleaner. The call quality is good. It doesn't show ads. For most people, that's a more persuasive reason to switch than anything about encryption. You can explain the security later, after they're already using it.

Enable disappearing messages. Open a Signal conversation, tap the contact name at the top, set disappearing messages to one week. This means messages automatically delete after seven days. It's not about hiding anything — it's about reducing the amount of data that exists if a device is ever compromised. Good security practice is reducing what's available,

not just protecting what's there.

Enable Registration Lock. In Signal, go to Settings → Account → Registration Lock. This prevents anyone from re-registering your Signal account on another device using your phone number — which is the Signal equivalent of SIM-swapping. It takes ten seconds.

Write in your field journal: who you moved to Signal, what resistance you encountered, what arguments worked. That last part matters more than you think — you're going to need those persuasion skills again.

Over a thousand people were identified after January 6, 2021, through a convergence of digital evidence. Facial recognition. Geofence warrants. Cell tower records. Citizen investigators who built databases from publicly posted footage. But the simplest vector — the one that required the least technical sophistication to exploit — was that people communicated in the open.

They posted on Facebook. They texted plans in unencrypted SMS. They live-streamed from inside the building. They took selfies and posted them with location tags. They messaged each other on platforms that logged every message, every contact, every group. When the subpoenas arrived, the platforms handed over everything, because everything was there to hand over.

The structural lesson is the same regardless of your politics: the people who were identified most quickly communicated as if no one was watching. The people who were identified more slowly — or not at all — practiced basic communications discipline. Encrypted messaging. No social media posts. No selfies. No live-streams.

Whatever your threat model says about who might access your communications and why — the technical response is the same. Encrypt the content. Minimize the metadata. Reduce what exists.

Your communications are now harder to read and harder to trace. That covers the digital channels between you and other people.

But it doesn't cover everything. Signal can't help you if your phone is broadcasting your location to a fake cell tower inside a briefcase. I'll explain that in the next chapter.

Summary

End-to-end encryption means only you and your recipient can read a message — not the company, not your carrier, not law enforcement. Signal is the gold standard: open-source, nonprofit, and when subpoenaed, it can produce almost nothing because it stores almost nothing. But encryption protects content, not metadata — and metadata (who you talk to, when, how often, from where) is often more revealing than message content itself.

Action Items

- Install Signal on your phone (free, available on iOS and Android)
- Move one important conversation to Signal — start with the person or group whose communications matter most to you
- Enable disappearing messages (tap contact name → set to 1 week)
- Enable Registration Lock (Settings → Account → Registration Lock)
- If people resist switching: lead with "it's a better app" (no ads, better group chats, good call quality) rather than surveillance concerns
- Record in your field journal: who you moved to Signal, what resistance you encountered, what persuasion worked

Case Studies & Citations

- **Signal subpoena responses** — When served with government subpoenas, Signal has produced only two data points: account creation date and last connection date. Published at signal.org/bigbrother.
- **Meta / WhatsApp government data requests** — Meta complied with approximately 77% of US government data requests in its most recent transparency report. Compliance involves metadata (contacts, timing, IP addresses, group memberships), not message content.
- **NSA bulk phone records collection (2013)** — Edward Snowden revealed the NSA's program collecting metadata on millions of phone calls under Section 215 of the Patriot Act. The legal basis relied on the position that metadata collection is less invasive than content collection.
- **General Michael Hayden on metadata** — The former NSA and CIA director publicly stated: "We kill people based on metadata." Describing how intelligence targeting relies on communication patterns rather than message content.
- **January 6 digital forensics (2021)** — Over 1,000 individuals identified through converging evidence including unencrypted social media posts, SMS messages, live-streams, and platform-stored data handed over in response to subpoenas. Illustrates the consequences of communicating without encryption or metadata awareness.
- **iCloud backup vulnerability** — Apple can access iCloud-backed-up messages when served with a warrant, unless the user has enabled Advanced Data Protection (end-to-end encryption for iCloud). Most users have not enabled this setting.

Templates, Tools & Artifacts

- **Signal** — Free, open-source, nonprofit encrypted messaging app. End-to-end encrypted content with minimal metadata collection. Available at signal.org.
- **Signal Registration Lock** — Prevents re-registration of your Signal account on another device using your phone number. Settings → Account → Registration Lock.
- **Disappearing messages** — Signal feature that automatically deletes messages af-

ter a set period (recommended: 1 week). Reduces data exposure if a device is compromised.

Key Terms

- **End-to-end encryption (E2EE)** — Encryption where messages are locked on the sender's device and only unlocked on the recipient's device. No intermediate party — not the app company, not the carrier, not the server — can read the content.
- **Metadata** — Data about communications rather than the content itself: who you talked to, when, how long, from where, how often. Often more revealing than message content and subject to weaker legal protections.
- **Content vs. metadata** — The critical distinction in communications security. Encryption protects content; minimizing what a platform collects protects metadata. Signal addresses both. WhatsApp addresses only content.
- **SIM-swapping** — An attack where someone transfers your phone number to their device (introduced in Chapter 4). Signal's Registration Lock is the defense against the Signal-specific version of this attack.

Chapter 6

The Watchers

I ended the last chapter by mentioning a briefcase-sized device that impersonates a cell tower. Let me describe what that actually means for your phone.

A Stingray is a device about the size of a carry-on suitcase. It broadcasts a signal that mimics a legitimate cell tower, and your phone connects to it automatically. Your phone doesn't ask you. It doesn't notify you. It connects to the strongest signal it can find, and the Stingray makes sure that's itself.

Once your phone connects, the operator can pull your IMSI number — the unique identifier for your SIM card — and your precise GPS location. Some newer versions can intercept call and text content. The critical thing to understand is that Stingrays are indiscriminate. They don't target one phone. They capture data from every phone within range. If you're standing at a protest, a courthouse, a church, a clinic — every person's phone in that area connects and identifies itself.

The ACLU has documented at least 75 law enforcement agencies in 27 states possessing these devices. That's almost certainly an undercount, because many agencies sign non-disclosure agreements with the manufacturers that prevent them from acknowledging they even own one. ICE deployed Stingrays at least 466 times between 2017 and 2019. The devices have been used at protests, near border crossings, and in routine investigations where no warrant was obtained.

That's one technology. Let me show you the rest.

What I'm going to lay out now is the surveillance infrastructure that already exists, is already deployed, and is already being used — in your city, on your roads, pointed at your face. I've spent the last several chapters teaching you to secure your individual digital life. This chapter is about what's watching you in the physical world, because the two aren't separate

— they feed the same databases.

License plate readers. Flock Safety operates automated license plate reader cameras in over 5,000 communities across 49 states. These cameras photograph the rear of every passing vehicle, read the plate, log the time and location, and store it in a searchable database. Flock's network performs over 20 billion scans per month. An EFF investigation of Flock's audit logs found that more than 3,900 law enforcement agencies logged over 12 million searches between December 2024 and October 2025.

Twelve million searches in ten months. Not investigations. Searches. Any officer with access to the system can type in a plate number and pull up everywhere that car has been within range of a camera.

The documented uses include tracking protest attendees, targeting Romani people with discriminatory searches, and — in one case out of Texas — an officer searching a nationwide network of over 83,000 cameras looking for a woman who had self-administered an abortion. Flock's newer product, Nova, integrates license plate data with information from data breaches and public records to build profiles of individuals without a warrant.

The cameras are solar-powered, mounted on poles, and most people drive past them every day without noticing.

Facial recognition. Clearview AI maintains a database of over 70 billion images scraped from the public internet — news sites, social media, anything with a face. Law enforcement agencies can upload a photo and search for matches across that entire database. Clearview signed a $10 million federal contract in September 2025 — their largest to date — and holds a separate $9.2 million contract with ICE. Customs and Border Protection has begun piloting the technology with licenses for agents at their National Targeting Center.

The accuracy question matters. NIST — the National Institute of Standards and Technology — tested 189 facial recognition algorithms in 2019 and found that many were 10 to 100 times more likely to produce a false positive match for Black and Asian faces compared to white faces. At least eight documented wrongful arrests have resulted from facial recognition misidentification in the US. All of the people wrongfully arrested were Black.

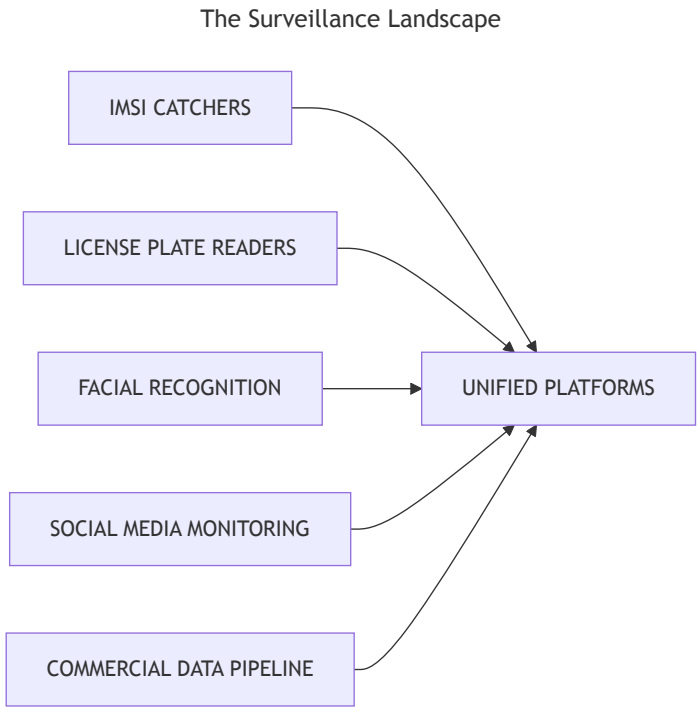
In 2020, NYPD used facial recognition to match Derrick Ingram's social media photos to protest footage. More than 50 officers surrounded his apartment. They deployed a drone. Amnesty International documented

over 2,700 instances of NYPD using facial recognition at Black Lives Matter protests that year.

That same year in Detroit, Robert Williams was arrested at his home in front of his family for a shoplifting he didn't commit. The facial recognition system had matched his driver's license photo to blurry surveillance footage of a different person. He was held for 30 hours. He later received a $300,000 settlement — but no amount of money erases being handcuffed in front of your children for something you didn't do.

Social media monitoring. Babel Street (from Chapter 2) built a product called Locate X and holds contracts with the Department of Justice, FBI, and other federal agencies for its surveillance platform, which searches across over 200 languages on 30-plus social media platforms. Dataminr — a company that monitors social media for law enforcement — sent the DC Metropolitan Police over 160,000 email alerts between June 2020 and May 2022 covering protests, including individual social media handles and bios. Meta sued Voyager Labs in 2023 for creating 55,000 fake accounts to scrape 1.2 million user profiles for law enforcement surveillance tools.

I need you to hold all of this together for a moment. License plate readers logging your movements. Facial recognition matching your face to a database of 70 billion images. Social media monitoring tools flagging your posts, your handles, your connections. Stingrays capturing your phone's identity when you walk past. The commercial surveillance pipeline from Chapter 2 selling your app data to anyone who pays.



These aren't separate systems. They feed the same databases, are queried by the same agencies, and are increasingly integrated by companies like Palantir into unified platforms that correlate all of it. Your license plate data, your face, your phone's location, your social media activity, your data broker profile — linked, searchable, and available without a warrant in most cases.

That convergence is the landscape. It's pervasive, near-invisible, and expanding every day.

If you've seen The Matrix Reloaded, you remember the Architect. He's not an agent. He doesn't chase anyone. He built the system — the entire architecture that makes chasing unnecessary. Every anomaly, every pattern, every deviation is already captured because the Matrix itself is the surveillance. The agents are an afterthought. The architecture does the work.

That's what you're looking at. Not a program that targets you. An architecture that captures everyone, and then lets operators query it after the fact. The cameras don't know you're interesting. The plate readers don't care where you're going. The facial recognition isn't hunting you

specifically. It doesn't need to. It already has your face, your plate, your phone, your posts — filed, indexed, and waiting for the moment someone decides to look.

The Architect didn't need to know which anomaly mattered. He just needed to make sure the system recorded all of them. That's the design principle behind everything I just described.

The most important thing you can do right now is understand the landscape before I start handing you countermeasures that require context to use correctly.

But do this: look up whether your city or county uses Flock Safety cameras. Search "[your city] Flock Safety" or "[your county] ALPR." You can also check the EFF's Street-Level Surveillance atlas for a broader picture of what technology your local police department has acquired.

Write down what you find in your field journal. You're building a map of your own environment now — not just your digital environment, but your physical one.

Everything I've just described is the infrastructure. By itself, infrastructure is inert — it does what the people operating it decide to do.

The next chapter is about history — specifically, about a program that did everything I just described, using 1960s technology, and got away with it for fifteen years before a congressional committee exposed it. If you want to know what this surveillance infrastructure looks like when it's used with intent against a democratic society's own citizens, the answer is already in the congressional record.

Summary

The physical surveillance infrastructure aimed at ordinary Americans includes automated license plate readers (20+ billion scans per month across 49 states), facial recognition systems (70+ billion scraped images, documented racial bias, wrongful arrests), cell-site simulators that capture every phone in range, and social media monitoring platforms tracking posts and connections across dozens of platforms. These systems aren't separate — they feed interconnected databases, are queried by the same agencies, and are increasingly integrated into unified platforms. Understanding this landscape is a prerequisite for using countermeasures effectively.

Action Items

- Search "[your city] Flock Safety" or "[your county] ALPR" to find out if your area uses automated license plate readers
- Check the EFF's Street-Level Surveillance atlas (atlas.eff.org) for a broader view of surveillance technology your local police have acquired
- Write what you find in your field journal — you're mapping your physical environment now, not just your digital one

Case Studies & Citations

- **Stingray / IMSI catchers** — The ACLU has documented at least 75 law enforcement agencies in 27 states possessing cell-site simulators. ICE deployed them at least 466 times between 2017 and 2019. Many agencies sign non-disclosure agreements with manufacturers preventing them from acknowledging ownership.
- **Flock Safety / ALPR** — Over 5,000 communities across 49 states. 20+ billion plate scans per month. EFF investigation of audit logs found 3,900+ agencies logged 12 million+ searches between December 2024 and October 2025. Documented misuse includes tracking protest attendees, discriminatory searches targeting Romani people, and a Texas officer searching 83,000+ cameras for a woman who had self-administered an abortion.
- **Flock Nova** — Flock's newer product integrating license plate data with data breach information and public records to build profiles without warrants.
- **Clearview AI** — Database of 70+ billion scraped images (per Clearview's own site, January 2026). $10 million federal contract signed September 2025 (largest to date). $9.2 million ICE contract signed 2025. CBP piloting with licenses at the National Targeting Center.
- **NIST facial recognition testing (2019)** — Tested 189 algorithms. Found many were 10–100x more likely to produce false positives for Black and Asian faces compared to white faces.
- **Wrongful arrests from facial recognition** — At least eight documented cases in the US as of 2026. All involved Black individuals. Includes Robert Williams (Detroit, 2020) — arrested in front of his family based on a mismatched driver's license photo, held for 30 hours, received $300,000 settlement.
- **Derrick Ingram (2020)** — NYPD used facial recognition to match his social media photos to protest footage. 50+ officers surrounded his apartment. Amnesty International documented 2,700+ NYPD facial recognition uses at Black Lives Matter protests that year.
- **Babel Street / Locate X** — Surveillance platform searching across 200+ languages on 30+ social media platforms. Contracts with DOJ, FBI, and other federal agencies.
- **Dataminr** — Sent DC Metropolitan Police 160,000+ email alerts between June 2020 and May 2022 covering protests, including individual social media handles and bios.
- **Meta v. Voyager Labs (2023)** — Meta sued Voyager Labs for creating 55,000 fake accounts to scrape 1.2 million user profiles for law enforcement surveillance tools.
- **Palantir** — Referenced as an integrator of multiple surveillance data streams into unified, queryable platforms.

Templates, Tools & Artifacts

- **EFF Street-Level Surveillance atlas** — Interactive map of surveillance technology acquired by local law enforcement agencies. Available at atlas.eff.org.
- **Field journal: physical environment map** — Record what surveillance infras-

tructure exists in your area: ALPR cameras, facial recognition use, social media monitoring contracts. This builds on the digital environment mapping from earlier chapters.

Key Terms

- **IMSI catcher / Stingray** — A device that mimics a cell tower, causing all phones within range to connect and identify themselves. Captures IMSI numbers (unique SIM card identifiers) and GPS locations. Some versions can intercept call and text content. "Stingray" is a brand name that has become the generic term.
- **ALPR (Automated License Plate Reader)** — Camera systems that photograph vehicle license plates, read the numbers, and log time and location in searchable databases. Often solar-powered and mounted on poles.
- **IMSI (International Mobile Subscriber Identity)** — The unique identifier associated with your SIM card. An IMSI catcher captures this to identify and locate your phone.
- **Clearview AI** — A facial recognition company that scraped the public internet to build a database of 70+ billion images. Sells access to law enforcement agencies for searching faces against the database.
- **NIST (National Institute of Standards and Technology)** — Federal agency that tests and evaluates technology standards, including facial recognition algorithm accuracy across demographics.
- **Palantir** — A data analytics company that integrates multiple surveillance and data streams into unified platforms used by government agencies. Named here as an example of how separate surveillance systems become interconnected.

Chapter 7

COINTELPRO Never Ended — It Just Got an Upgrade

On December 4, 1969, at 4:45 in the morning, fourteen Chicago police officers armed with shotguns and a submachine gun kicked down the door of a West Side apartment. Inside, several members of the Black Panther Party were asleep.

The officers fired over 90 rounds into the apartment. The occupants fired once — a single shot from Mark Clark's gun, likely discharged reflexively as he was hit. Clark was killed at the door. Fred Hampton, the 21-year-old chairman of the Illinois Black Panther Party, never left his bed. He'd been drugged earlier that evening by William O'Neal — an FBI informant who had become Hampton's bodyguard. O'Neal had drawn the floor plan of the apartment for the agents who planned the raid. According to witnesses, an officer stood over Hampton's unconscious body, asked if he was still alive, and two shots were fired into his head. "He's good and dead now," one officer said.

Hampton's fiancée, eight months pregnant, had been lying next to him.

O'Neal received a $300 bonus from the FBI for his work.

COINTELPRO — the Counter Intelligence Program — ran from 1956 to 1971. It was not a conspiracy theory. It was a documented FBI operation exposed by the Church Committee, a Senate investigation whose findings are part of the congressional record. The committee's own words: COINTELPRO was "a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights of speech and association."

The tactics were systematic. I'm going to name them specifically, because each one has a modern equivalent.

Infiltration. The FBI planted informants and undercover agents inside organizations. O'Neal inside the Black Panthers is the most famous case, but there were hundreds. The purpose wasn't intelligence-gathering — it was disruption. Informants were tasked with creating internal conflicts,

encouraging illegal activity that could be used for prosecution, and identifying leaders for targeting.

Disinformation. The FBI fabricated letters between organizations to provoke distrust and violence. They sent forged communications designed to look like they came from rival groups, planted false stories in newspapers, and created fake leaflets attributed to organizations they wanted to discredit. The goal was to make groups turn on each other.

Bad-jacketing. This is the tactic I think is most likely to resurface at scale. Bad-jacketing means falsely labeling loyal members of an organization as informants. The FBI would circulate rumors, fabricate evidence, and create documents suggesting that trusted members were actually government agents. The resulting paranoia destroyed organizations from within more effectively than any external pressure could.

Direct targeting of leaders. In 1964, the FBI sent Martin Luther King Jr. an anonymous letter accompanied by surveillance recordings, urging him to commit suicide before his "filthy, abnormal fraudulent self is bared to the nation." The letter implied he had 34 days to act. This was not a rogue agent. It was approved by senior FBI leadership under a program that J. Edgar Hoover described as targeting the "greatest threat to the internal security of the country" — his characterization of the Black Panther Party. King was assassinated 4 years later.

The program didn't target one group. COINTELPRO operations were conducted against the Southern Christian Leadership Conference, the Student Nonviolent Coordinating Committee, the American Indian Movement, the Puerto Rican independence movement, the New Left, antiwar organizations, feminist groups, and environmental activists. The common thread wasn't ideology. It was dissent.

In 1975, the Church Committee exposed all of this. Senator Frank Church warned, on national television, that the NSA's surveillance capabilities could "at any time be turned around on the American people, and no American would have any privacy left." He was talking about the technology of the 1970s.

The committee's findings led to reforms: Executive Order 12333 restricting domestic intelligence activities, the Foreign Intelligence Surveillance Act creating a court to oversee surveillance warrants, congressional intelligence committees established. For a period, the infrastructure of domestic surveillance was constrained by law.

Then those constraints were systematically dismantled. The PATRIOT Act, passed six weeks after September 11, 2001, expanded the government's surveillance authorities in ways the Church Committee reforms had specifically tried to prevent. In 2013, Edward Snowden revealed the scope of what had been built: PRISM collected data directly from servers of nine major internet companies. Upstream collection tapped the fiber optic cables carrying internet traffic. The system Senator Church had warned about, built exactly as he predicted, operated in secret for years.

The pattern is the same every time. Capability is built for one purpose. Mission creep expands its use. Abuse follows. This isn't cynicism — it's the documented historical record, exposed by the government's own investigations.

If you've seen *The Hunger Games*, you know President Snow's playbook. Surveillance. Infiltration. Turning districts against each other. Keeping the population afraid, divided, and convinced that resistance is futile. Snow didn't need to control every citizen — he needed to control the infrastructure that made control possible. The Peacekeepers, the Capitol's surveillance network, the televised spectacle designed to make rebellion look hopeless — these weren't improvisations. They were part of the architecture.

In 2025, DOGE accessed Social Security Administration data covering hundreds of millions of Americans. Court filings later revealed that DOGE employees improperly shared sensitive personal data on outside servers and circumvented IT security rules — and that the government had misrepresented the extent of access in its own testimony. IRS data was shared with ICE before courts intervened. Palantir contracted to build a system called "ImmigrationOS" that compiles government databases into a unified targeting and enforcement platform. A privacy law professor called this "the demolition of the Watergate-era safeguards that were intended to keep databases separated."

Dozens of lawsuits have been filed challenging DOGE's data access across multiple federal agencies — Treasury, OPM, SSA, IRS, the Department of Labor, and others. The Supreme Court, in a case that reached it on the emergency docket, ultimately allowed DOGE access to Social Security records to continue while litigation proceeds. The legal battles are ongoing, the outcomes uncertain.

I'm going to say something carefully here. Whether you support the

current administration's goals or oppose them, the infrastructure being built will be inherited by every administration that follows. That's the lesson COINTELPRO teaches. The program survived the transition from Eisenhower to Kennedy to Johnson to Nixon — four presidents across both parties, none of whom shut it down. The capability outlived the people who built it and was used by every successor for their own purposes.

The surveillance infrastructure I mapped in the last chapter — the license plate readers, the facial recognition, the social media monitoring, the commercial data pipeline — is the modern equivalent of what COINTELPRO had in the 1960s, except orders of magnitude more powerful, more pervasive, and more automated. Snow's playbook, with better tools.

This isn't uniquely American.

In the UK, the Undercover Policing Inquiry has documented that over 139 undercover officers infiltrated more than 1,000 political groups across four decades. Officers formed intimate relationships with activists, fathered children with them, then disappeared. Of the hundreds of groups infiltrated, only three were later found to be justified on public safety grounds. Three out of a thousand.

This matters because the reflex when hearing about COINTELPRO is to categorize it as a dark chapter that ended. It didn't end. The tactics adapted. The technology improved. And the targets — people exercising their rights to organize, protest, and dissent — remain the same.

The Church Committee is proof that exposure and reform are possible. The congressional record exists. The findings were published. Laws were passed. The system responded to democratic pressure, even if those reforms were later eroded.

That's the pattern you need to recognize: capability leads to abuse, but exposure leads to accountability — if people know what to look for and insist on transparency.

Two things.

First: read the ACLU Know Your Rights overview. It's at aclu.org/know-your-rights. It covers interactions with law enforcement, immigration agents, and protests. Read it the way you'd read a manual for lifesaving equipment you hope you never need to use.

Second: memorize four phrases. Write them in your field journal.

"Am I free to go?"

"I do not consent to this search."

"I am exercising my right to remain silent."

"I want to speak to a lawyer."

These are not magic words. They don't prevent anything. What they do is establish a legal record. If your rights are violated after you've clearly stated them, that matters in court. If you haven't stated them, it becomes much harder to demonstrate that a violation occurred. The phrases are a tool — a simple one, free, requiring nothing but the willingness to say them out loud when it matters.

History provides examples. Your threat model focuses on what's worth protecting. But there's a gap between what you think is private and what anyone with a search engine can find out about you.

Come back this evening. We're going on a spy mission.

Summary

COINTELPRO was a documented FBI program that ran from 1956 to 1971, using infiltration, disinformation, bad-jacketing, and direct targeting of leaders to suppress dissent. The Church Committee exposed it. Reforms followed — and were later dismantled by the PATRIOT Act and expanded surveillance authorities revealed by Snowden. The same pattern — capability built, mission creep, abuse — is repeating now with DOGE accessing government databases covering hundreds of millions of Americans, IRS-ICE data sharing, and Palantir building unified surveillance platforms. The infrastructure being built today will be inherited by every future administration.

Action Items

- Read the ACLU Know Your Rights overview at aclu.org/know-your-rights — covers interactions with law enforcement, immigration agents, and protests
- Memorize four phrases and write them in your field journal: "Am I free to go?" / "I do not consent to this search." / "I am exercising my right to remain silent." / "I want to speak to a lawyer."
- These phrases establish a legal record — they don't prevent anything, but they matter in court if your rights are violated

Case Studies & Citations

- **Fred Hampton assassination (December 4, 1969)** — 21-year-old chairman of the Illinois Black Panther Party killed in a pre-dawn raid by Chicago police coordinating with the FBI. William O'Neal, an FBI informant who had become Hampton's bodyguard, drugged Hampton and provided the floor plan to agents. Officers fired over 90 rounds; occupants fired once. Mark Clark also killed. O'Neal received a $300 bonus.

- **COINTELPRO (1956–1971)** — Documented FBI program exposed by the Church Committee. Senate investigation described it as "a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights of speech and association." Targeted the SCLC, SNCC, the American Indian Movement, the Puerto Rican independence movement, the New Left, antiwar organizations, feminist groups, and environmental activists.
- **FBI letter to Martin Luther King Jr. (1964)** — Anonymous letter accompanied by surveillance recordings, urging King to commit suicide. Approved by senior FBI leadership. Implied he had 34 days to act.
- **COINTELPRO tactics with modern equivalents** — Infiltration (undercover officers in protest movements). Disinformation (fabricated communications, planted stories). Bad-jacketing (labeling loyal members as informants to destroy trust). Direct targeting of leaders.
- **Church Committee (1975)** — Senate investigation that exposed COINTELPRO. Senator Frank Church warned on national television that NSA surveillance capabilities could "at any time be turned around on the American people." Led to Executive Order 12333, FISA, and congressional intelligence oversight.
- **PATRIOT Act (2001)** — Passed six weeks after September 11. Expanded surveillance authorities the Church Committee reforms had tried to prevent. Section 215 used to justify bulk phone records collection.
- **Edward Snowden revelations (2013)** — Revealed PRISM (data collection from nine major internet companies) and upstream collection (tapping fiber optic cables). Documented that the surveillance system Church had warned about had been built and operated in secret.
- **DOGE and SSA data access (2025–2026)** — DOGE accessed Social Security Administration data covering hundreds of millions of Americans. Court filings revealed DOGE employees improperly shared sensitive data on outside servers, circumvented IT rules, and that the government misrepresented the extent of access in testimony. Multiple federal courts issued injunctions; the Supreme Court stayed one injunction allowing access to continue. Dozens of lawsuits filed across multiple agencies.
- **Palantir / ImmigrationOS (2025)** — $30 million ICE contract to build a unified platform for targeting and enforcement prioritization, self-deportation tracking, and immigration lifecycle management. Integrates data from multiple government databases. Prototype delivered September 2025.
- **IRS-ICE data sharing (2025)** — IRS data shared with immigration enforcement before courts intervened.
- **UK Undercover Policing Inquiry** — 139+ undercover officers infiltrated 1,000+ political groups over four decades. Officers formed intimate relationships with activists and fathered children. Of hundreds of groups infiltrated, only three were later justified on public safety grounds.

Templates, Tools & Artifacts

- **ACLU Know Your Rights** — Overview of rights during interactions with law enforcement, immigration agents, and at protests. Available at aclu.org/know-your-rights.
- **Four phrases for legal encounters** — "Am I free to go?" / "I do not consent to this search." / "I am exercising my right to remain silent." / "I want to speak to a lawyer." Establishes a legal record; does not prevent actions but creates documentation if rights are violated.

Key Terms

- **COINTELPRO (Counter Intelligence Program)** — FBI program (1956–1971) that used infiltration, disinformation, bad-jacketing, and leader targeting to suppress domestic dissent. Exposed by the Church Committee. Findings are part of the congressional record.
- **Bad-jacketing** — The tactic of falsely labeling loyal members of an organization as informants to create paranoia and internal collapse. Used extensively by the FBI against civil rights and protest organizations. Also referred to as "snitch-jacketing."
- **Church Committee** — Senate committee (1975) that investigated and exposed COINTELPRO and other intelligence abuses. Led to significant surveillance reforms including FISA and congressional oversight committees.
- **FISA (Foreign Intelligence Surveillance Act)** — Law creating a court to oversee surveillance warrants, established as a reform after the Church Committee revelations. Section 702, added later, authorized broader collection from internet companies without individual warrants.
- **DOGE (Department of Government Efficiency)** — Entity established by executive order in January 2025. Gained or sought access to sensitive databases across multiple federal agencies. Subject of dozens of federal lawsuits alleging Privacy Act and constitutional violations.
- **ImmigrationOS** — Palantir-built platform for ICE that integrates government databases for immigration enforcement targeting, tracking, and case management. $30 million contract awarded April 2025.

Chapter 8

You Are Not Hard to Find

Open a browser. Go to TruePeopleSearch.com. Type in your name and your state.

I'll wait.

If your experience is like most people's, you just found your home address, your phone number, your age, your previous addresses, the names of your relatives, and possibly your estimated income — listed publicly, searchable by anyone, for free. Spokeo.com will show you similar information, often with your email addresses and social media profiles attached. There are hundreds of these sites. They aggregate data from public records, commercial databases, and data brokers — the same pipeline I described in Chapter 2, except this is the consumer-facing end. The data broker sells your profile wholesale. The people search site sells it retail, one lookup at a time, to anyone who types your name.

Now do this: open a new tab and Google yourself. Try your full name plus your city. Then your name plus your phone number. Then your name plus your email address.

Look at what comes back. Look at the images. Look at how many versions of your digital identity exist across how many sites, and notice how much of it you didn't put there.

This is what you look like to anyone who wants to find you. An abusive ex-partner. A stalker. A doxxer. An employer running an off-the-books background check. A data broker building a profile. A law enforcement officer doing preliminary research before there's any investigation. The information is there, it's free, and it takes less time to find than it took you to read the last paragraph.

Most people dramatically underestimate their own exposure. Not because they're careless — because the gap between what you think is private

and what's actually findable has been widening for two decades, and no one sends you a notification when your home address appears on a new people-search site.

Data brokers re-aggregate your information every three to six months. Even if you've never signed up for a data broker site, you're on them. They pull from public records — voter registration, property records, court filings, professional licenses — and from the commercial surveillance pipeline. Every time you opt out, you're removing one copy. The sources keep generating new ones.

This sounds discouraging. It shouldn't be. Here's why.

Consumer Reports ran a study on data broker opt-outs and found that manual removals were at least as effective as paid services — and in some cases more effective, because paid services automate a process that some brokers are better at blocking than the manual route. The opt-outs work. They're free. They take time. And yes, you'll need to redo them periodically. Think of it the way you think about changing your oil — it's maintenance, not a one-time fix.

Three things. All today.

First: search yourself on TruePeopleSearch and Spokeo. You've probably already done TruePeopleSearch. Do Spokeo too. Write down exactly what each site has on you. This goes in your field journal — it's your exposure baseline.

Second: begin the opt-out process. Both sites have removal processes. For TruePeopleSearch, scroll to the bottom of the homepage and click "Do Not Sell or Share My Personal Information," then follow the opt-out form. For Spokeo, go to spokeo.com/optout, enter the URL of your listing, provide an email address, and confirm. Use a disposable email if you have one — data brokers have been known to add the email you use for opt-outs back into their databases.

After those two, do the same for Whitepages, BeenVerified, and Radaris. Between those five, you'll have covered the largest people-search sites. The process for each takes five to ten minutes.

Third: set up Google "Results About You." Google has a tool that lets you request removal of search results containing your personal contact information — phone number, home address, email. Go to myactivity.google.com/results-about-you or search "Google Results About You" to find it. It's not comprehensive, but it's free and it flags new results as they appear. Think of it

as an early warning system for your exposure.

If you're Tier 2 or 3 in your threat model, run the free Optery scan at optery.com. It searches over a thousand data broker sites at once and shows you everywhere your information appears. The free scan tells you where you are. Their paid service handles removals, but you can use the scan results to do manual opt-outs yourself.

Record everything in your field journal. What you felt, what you found, where, what you've requested removal from, and what's still outstanding. You're going to check back in a few months.

Let me tell you about a trail of breadcrumbs.

In May 2020, a woman was captured on news footage setting two Philadelphia police cars on fire during a protest. She was wearing a mask, goggles, and a distinctive T-shirt. She thought she was anonymous.

FBI agents identified the T-shirt — "Keep the immigrants, deport the racists" — and found the Etsy shop that sold it. On the Etsy listing, a reviewer from Philadelphia had left a five-star review under a username. Agents searched that username and found it on Poshmark, a clothing resale site, where the display name was "lore-elisabeth." They searched that name and found a LinkedIn profile for a massage therapist in Philadelphia. Her employer's website had videos showing her at work. In the videos, agents spotted a distinctive tattoo on her forearm — the same tattoo visible in the protest footage.

Lore-Elisabeth Blumenthal was arrested and eventually sentenced to two and a half years in federal prison. The entire identification chain started with a reused username on a shopping site.

No facial recognition. No surveillance technology. No warrants for data. Just the connections between accounts that shared identifiers — a username, a name, a location — because no one thinks about how their Etsy reviews connect to their LinkedIn page connects to their employer's website connects to their physical body.

That's what OSINT is. Open-source intelligence — the practice of building a complete picture of someone from publicly available information. It's what investigators do. It's what doxxers do. It's what data brokers automate at scale. And the raw material for all of it is the connections between your accounts, your names, your handles, and your patterns.

If you've seen *Fight Club*, you remember Project Mayhem's fantasy: blow up the credit card companies, erase the debt record, reset everyone to zero.

Tyler Durden wanted to destroy the system that tracked you. It's a satisfying fantasy — but it's a fantasy. The records can't be destroyed. They regenerate. The data brokers re-aggregate. The public records refresh. New connections form every time you create an account, leave a review, or appear in someone else's photo.

The real version of Project Mayhem isn't erasure. It's management. You can't blow up the building where your data lives, because your data lives in a thousand buildings. What you can do is reduce your exposure, break the connections between identities, and make the trail harder to follow. That's what the opt-outs are. That's what username discipline is. Not a reset — ongoing maintenance of the gap between your real life and your findable life.

Look at your own accounts. How many of your usernames are the same across platforms? How many connect your real name to accounts you'd rather keep separate? If someone started with your LinkedIn and worked outward — the way those agents worked outward from Blumenthal's — what would they find? How many steps between your professional identity and your private one?

You don't need to fix all of this tonight. But you need to see it. The next chapter addresses the window you're looking through right now — your browser. It's a two-way window.

`Summary`

Your personal information — home address, phone number, relatives' names, estimated income — is almost certainly listed publicly on people-search sites, searchable by anyone for free. This is the consumer-facing end of the data broker pipeline from Chapter 2. Manual opt-outs work (Consumer Reports found them at least as effective as paid services), but data brokers re-aggregate every 3–6 months, making this ongoing maintenance. OSINT — open-source intelligence — can build a complete picture of someone from publicly available connections between accounts, as the Blumenthal case demonstrates. Reducing exposure means breaking connections between identities and maintaining the gap between your real life and your findable life.

`Action Items`

- Search yourself on TruePeopleSearch.com and Spokeo.com — write down exactly what each site has on you (this is your exposure baseline)
- Begin opt-outs: TruePeopleSearch (bottom of homepage → "Do Not Sell or Share My Personal Information"), Spokeo (spokeo.com/optout), then Whitepages,

BeenVerified, and Radaris — five to ten minutes each
- Use a disposable email for opt-outs if possible (brokers have been known to add opt-out emails back into their databases)
- Set up Google "Results About You" (myactivity.google.com/results-about-you) — flags new results containing your personal contact information
- Google yourself: full name + city, name + phone number, name + email address
- Tier 2/3: Run the free Optery scan at optery.com (searches 1,000+ data broker sites)
- Audit your usernames: how many are the same across platforms? How many connect your real name to accounts you'd rather keep separate?
- Record everything in your field journal — what you found, where, what you've requested removal from, what's outstanding

Case Studies & Citations

- **Lore-Elisabeth Blumenthal (Philadelphia, 2020)** — Captured on footage setting two police cars on fire during a protest while wearing a mask and goggles. FBI traced her through: distinctive T-shirt → Etsy shop → reviewer username → Poshmark ("lore-elisabeth") → LinkedIn profile → employer website videos → forearm tattoo match to protest footage. Sentenced to two and a half years. No facial recognition, surveillance technology, or warrants required — only publicly available connections between accounts sharing identifiers.
- **Consumer Reports data broker opt-out study** — Found manual removals at least as effective as paid services, and in some cases more effective because paid services automate processes that some brokers are better at blocking.
- **Data broker re-aggregation cycle** — Brokers rebuild profiles from public records and commercial data every 3–6 months. Sources include voter registration, property records, court filings, professional licenses, and the commercial surveillance pipeline.

Templates, Tools & Artifacts

- **TruePeopleSearch** — Free people-search site. Opt-out: scroll to bottom of homepage → "Do Not Sell or Share My Personal Information."
- **Spokeo** — Free people-search site. Opt-out: spokeo.com/optout → enter listing URL → provide email → confirm.
- **Whitepages, BeenVerified, Radaris** — Additional major people-search sites. Each has its own opt-out process; five to ten minutes per site.
- **Google "Results About You"** — Tool for requesting removal of search results containing your personal contact information. Available at myactivity.google.com/results-about-you. Free; flags new results as they appear.
- **Optery** — Free scan searches 1,000+ data broker sites. Paid tier handles removals; free tier provides results for manual opt-outs. Available at optery.com.
- **Self-OSINT audit** — Google yourself (name + city, name + phone, name + email). Check username reuse across platforms. Map connections between professional and private identities. Record exposure baseline in field journal.

Key Terms

- **OSINT (Open-Source Intelligence)** — The practice of building a complete picture of someone from publicly available information: social media, people-search sites, public records, employer websites, review platforms. Used by investigators, doxxers, and data brokers. The Blumenthal case illustrates the method.
- **People-search sites** — Consumer-facing websites that aggregate personal information from public records and data brokers. Display home addresses, phone

numbers, relatives' names, and more. Free to search; opt-outs available but require periodic maintenance.

- **Data broker re-aggregation** — The cycle by which data brokers rebuild profiles from source data every 3–6 months, even after opt-outs. Makes data removal an ongoing maintenance task rather than a one-time fix.
- **Username reuse** — Using the same username across multiple platforms, creating traceable connections between accounts. A primary vector for OSINT identification, as demonstrated in the Blumenthal case.
- **Exposure baseline** — A record of what personal information is currently findable about you online. Established by searching yourself and documenting results. Used to measure whether opt-outs and other mitigations are working.

Chapter 9

Your Browser Is a Fingerprint

If you think incognito mode protects you, it doesn't.

Private browsing does one thing: it hides your activity from other people who use your device. That's it. Your ISP still sees every site you visit. Websites still see your IP address. And your browser — the specific combination of your plugins, your fonts, your screen resolution, your language settings, your hardware — is a fingerprint nearly as unique as the one on your thumb.

If you've read *Through the Looking-Glass*, you remember the moment Alice steps through the mirror and discovers that everything on the other side is reversed — familiar but wrong, watching her as much as she's watching it. Your browser is that mirror. You think you're looking through a window at the internet. The internet is looking back through that same window at you — reading your configuration, cataloging your fingerprint, tracking your movement from site to site. Incognito mode is a curtain on your side of the glass. It doesn't change what's visible from the other side.

Go to coveryourtracks.eff.org. Run the test. It takes thirty seconds.

Look at the result. Look at how many bits of identifying information your browser broadcasts to every website you visit. Most browsers are unique among hundreds of thousands of samples. You're not anonymous. You're wearing a name tag you didn't know you had on.

That fingerprint follows you. When you visit a news site, a shopping site, a porn site, a political forum — the trackers embedded on those pages read your fingerprint and correlate your visits across them. They don't need cookies. They don't need you to log in. Your browser configuration is enough.

This is the technical reality behind those ads that follow you around the internet. But it's not just ads. In 2020, Denver police had no suspects in a fatal arson. They obtained a reverse keyword warrant — an order

requiring Google to reveal everyone who had searched for the address of the house in the fifteen days before the fire. Google produced a list. Police identified three teenagers. One of them, Gavin Seymour, was charged and eventually convicted.

The Colorado Supreme Court upheld the evidence in 2023 — the first state high court to rule on reverse keyword warrants. The court acknowledged the warrant was "constitutionally defective" but let the evidence stand under a good-faith exception. Your search history is evidence. Searching while signed into Google makes you identifiable.

Three things. All today.

Install uBlock Origin on Firefox. Not Chrome — Google removed uBlock Origin from the Chrome Web Store in late 2024 as part of its Manifest V3 transition, and permanently disabled all remaining Manifest V2 extensions in mid-2025. A limited version called uBlock Origin Lite exists for Chrome, but it blocks significantly less. If you're still using Chrome as your primary browser, this is a reason to switch. Firefox still supports the full extension and has committed to keeping it. uBlock Origin blocks trackers, ads, and known malicious domains. It is free and open-source.

Switch your default search engine to DuckDuckGo. DuckDuckGo doesn't log your searches. When you search on Google, your query is tied to your account, your IP address, your device, and your browsing profile. DuckDuckGo processes the query and returns results without recording who asked. It's not perfect — it pulls results from Bing — but the privacy difference is structural.

Test your browser fingerprint at coveryourtracks.eff.org — if you haven't already. Record the result in your field journal. Then install uBlock Origin, and run the test again. Compare.

If you're Tier 2 or 3 in your threat model, go further. Switch to Firefox if you haven't already. Enable Enhanced Tracking Protection in strict mode — it's in Settings → Privacy & Security. Try Firefox Multi-Account Containers, which lets you isolate different activities into separate containers so your banking session can't see your social media cookies. Enable DNS over HTTPS — in Firefox, go to Settings → Privacy & Security → scroll to DNS over HTTPS and select "Max Protection." This encrypts your DNS queries so your ISP can't see which domains you're visiting.

A note about VPNs, because I know you're wondering.

A VPN encrypts your internet traffic between your device and the VPN server. This hides your browsing from your ISP and your local network. It does not make you invisible. The VPN provider can see your traffic instead of your ISP — so you're choosing who to trust, not eliminating trust. VPNs matter most on public Wi-Fi, in situations where you don't trust your network, or when you want to prevent your ISP from logging the sites you visit.

If you're going to use one, use Mullvad or ProtonVPN. Mullvad doesn't require an email address to sign up — you get a random account number. You can pay with cash mailed in an envelope. ProtonVPN is based in Switzerland, has a free tier, and integrates with other Proton services. Both have been independently audited. Both have no-log policies that have held up under legal pressure. Most of the VPNs you see advertised online are owned by companies you should not trust with your traffic.

You can now see more clearly how you're tracked — through your location, your data, your passwords, your messages, your identity, and your browser. But there's a skill that matters as much as all of these combined, and it has nothing to do with technology.

It's about what you believe. The most sophisticated surveillance infrastructure in history is less dangerous than a population that can't tell truth from fabrication.

Summary

Incognito mode only hides activity from other users of your device — your ISP, websites, and trackers can still see everything. Your browser's unique combination of settings (plugins, fonts, resolution, hardware) creates a fingerprint that tracks you across sites without cookies or logins. Reverse keyword warrants can compel search engines to reveal who searched for specific terms. The practical defenses: Firefox with uBlock Origin (not Chrome — Google removed full uBlock Origin support in 2024–2025), DuckDuckGo as default search, and for higher threat models, Enhanced Tracking Protection, Multi-Account Containers, and DNS over HTTPS. VPNs shift trust from your ISP to the VPN provider — Mullvad and ProtonVPN are the recommendations.

Action Items

- Test your browser fingerprint at coveryourtracks.eff.org — record the result in your field journal
- Install uBlock Origin on Firefox (free, open-source — blocks trackers, ads, and malicious domains)

- If still using Chrome as primary browser, switch to Firefox — Chrome no longer supports full uBlock Origin
- Switch default search engine to DuckDuckGo (doesn't log searches)
- Install uBlock Origin, then re-run the fingerprint test and compare results
- Tier 2/3: Switch to Firefox if you haven't already; enable Enhanced Tracking Protection (strict mode) in Settings → Privacy & Security; try Firefox Multi-Account Containers; enable DNS over HTTPS (Settings → Privacy & Security → DNS over HTTPS → "Max Protection")

Case Studies & Citations

- **People v. Seymour (Colorado, 2020/2023)** — Denver police obtained a reverse keyword warrant requiring Google to reveal everyone who searched for a specific address in the fifteen days before a fatal arson. Three teenagers identified; Gavin Seymour charged and convicted. Colorado Supreme Court upheld the evidence in 2023 — first state high court to rule on reverse keyword warrants. Court acknowledged the warrant was "constitutionally defective" but let evidence stand under good-faith exception.
- **Google Manifest V3 transition (2024–2025)** — Google removed uBlock Origin from the Chrome Web Store in late 2024 and permanently disabled all remaining Manifest V2 extensions in mid-2025. uBlock Origin Lite (Manifest V3 compliant) exists but blocks significantly less. Firefox committed to continued Manifest V2 support.
- **Browser fingerprinting** — EFF's Cover Your Tracks tool demonstrates that most browsers are unique among hundreds of thousands of samples based on plugins, fonts, screen resolution, language settings, and hardware configuration. Trackers use this fingerprint to correlate visits across sites without cookies or login.

Templates, Tools & Artifacts

- **Cover Your Tracks (EFF)** — Browser fingerprint test at coveryourtracks.eff.org. Shows how many bits of identifying information your browser broadcasts. Run before and after installing uBlock Origin to compare.
- **uBlock Origin** — Free, open-source browser extension that blocks trackers, ads, and malicious domains. Full version available on Firefox (recommended) and Brave. Chrome limited to uBlock Origin Lite (reduced functionality).
- **DuckDuckGo** — Search engine that doesn't log searches or tie queries to user profiles. Pulls results from Bing. Privacy difference from Google is structural, not cosmetic.
- **Firefox Multi-Account Containers** — Extension that isolates browsing activities into separate containers (e.g., banking separate from social media). Prevents cross-site cookie tracking between contexts.
- **DNS over HTTPS** — Firefox setting that encrypts DNS queries, preventing your ISP from seeing which domains you visit. Enable in Settings → Privacy & Security → DNS over HTTPS → "Max Protection."
- **Mullvad VPN** — No email required to sign up (random account number). Accepts cash payment by mail. Independently audited. No-log policy held up under legal pressure.
- **ProtonVPN** — Swiss-based. Free tier available. Integrates with Proton Mail and other Proton services. Independently audited. No-log policy held up under legal pressure.

Key Terms

- **Browser fingerprinting** — The practice of identifying users by the unique combination of their browser's configuration: plugins, fonts, screen resolution, language settings, hardware. Nearly as unique as a physical fingerprint. Does not require cookies or login. Testable at coveryourtracks.eff.org.
- **Reverse keyword warrant** — A court order requiring a search engine to reveal all users who searched for specific terms within a given timeframe. Used in the Seymour case (2020). The Colorado Supreme Court was the first state high court to rule on their admissibility (2023).
- **Manifest V3** — Google's updated extension framework for Chrome, which restricts the capabilities of ad blockers and privacy tools. Caused the removal of full uBlock Origin from Chrome. Firefox is not affected.
- **VPN (Virtual Private Network)** — Encrypts internet traffic between your device and a VPN server, hiding browsing from your ISP and local network. Shifts trust from ISP to VPN provider — does not eliminate the need for trust. Most useful on public Wi-Fi or when ISP logging is a concern.
- **DNS over HTTPS** — Encrypts the domain name system queries your browser makes, preventing your ISP from seeing which websites you visit. Available in Firefox under Privacy & Security settings.

Chapter 10

Seeing Through the Noise

Before I teach you anything in this chapter, I want you to do something.

Open whatever social media platform you use most. Scroll until you find a claim that makes you feel something — anger, fear, vindication, hope. Something shared by someone you follow. Something that feels true.

Now stop. Don't share it. Don't react to it. Just sit with it and write down exactly what it claims, who originally made the claim, and what evidence is presented.

I'll come back to this.

Every skill I've covered so far has been about your data, your devices, your digital footprint. This chapter is different. This one is about your mind.

Information integrity is a core survival skill — not because misinformation is new, but because the tools for producing and distributing it are now cheaper, faster, and more convincing than at any point in history. A voice can be cloned from a few seconds of audio. AI-generated text is increasingly indistinguishable from human writing. Video can be fabricated with consumer-grade tools. And the same data broker ecosystem I described in Chapter 2 — the one that profiles and sells your attention — feeds you content calibrated to keep you engaged, not informed.

A 2018 MIT study examining over 126,000 stories spread on Twitter found that falsehoods were 70% more likely to be retweeted than true stories, and reached their first 1,500 people six times faster. A 2024 study published in *Science* found that misinformation sources evoke more outrage than trustworthy sources, and that outrage facilitates sharing — people will share content they know is inaccurate if it signals their moral position or group loyalty. That's not a platform failure. That's the business model working exactly as designed.

The Brennan Center for Justice obtained 160,000 email alerts that Dataminr — a social media monitoring company with access to the platform formerly known as Twitter's full data stream — sent to DC police over a two-year period. The alerts tracked planned demonstrations, individual protest organizers, the movements of marches in real time. One alert included the social media profile of a recent college graduate with fewer than 100 followers who had shared an event announcement.

That monitoring infrastructure runs on a firehose of content, and the content it processes most efficiently is the content that generates the most engagement — which is the content that triggers the strongest emotional responses. The surveillance infrastructure and the misinformation pipeline are not separate systems. They feed each other. Outrage produces data. Data enables targeting. Targeting produces more outrage.

If you can be manipulated into clicking, sharing, or believing false information, you can be manipulated into compromising your security. A convincing phishing email works because it triggers an emotional response — urgency, fear, curiosity — that overrides the careful habits you've been building. Misinformation works the same way at scale.

In *Ender's Game*, there's a subplot most people forget. Between the Battle Room exercises — the tactical training everyone remembers — Ender plays something called the Mind Game. It's a psychological simulation that adapts to the player, presenting scenarios with no obvious right answer. The game watches how you respond. It learns what makes you react. And at a critical point, Ender can no longer tell whether the game is testing him or he's testing it — whether he's inside a simulation or something real.

That's the information environment you're living in right now. Content designed to provoke a reaction. Systems that learn what makes you click. And a diminishing ability to tell what's real from what's been engineered to feel real. The Mind Game was never about winning. It was about whether you could maintain your judgment when everything around you was designed to manipulate it.

The difference is that Ender didn't have a method. You do.

Here's the framework. It's called SIFT, developed by digital literacy researcher Mike Caulfield. Four steps.

Stop. Before you share, react to, or act on a piece of information, pause. That's it. The single most effective intervention against misinformation is

a thirty-second delay between encountering a claim and doing anything with it.

Investigate the source. Who originally published this? Not who shared it — who made the claim? A credible person citing their expertise? A website you've never heard of? An account created last month? Don't evaluate the claim yet. Evaluate the claimant.

Find better coverage. If the claim is real, other sources will be reporting it. Search for the claim — not the article, the underlying claim — and see who else is covering it. If a major event is reported by only one source or one political orientation, that's a signal. If you can find the claim reported across multiple outlets with different perspectives, the core facts are more likely solid even if the framing varies.

Trace claims to their origin. If a claim cites a study, find the study. If it quotes a person, find the original quote in context. If it references a document, find the document. Most misinformation isn't fabricated from nothing — it's real information stripped of context, reframed, or selectively quoted. Following the chain back to the original source often reveals what was left out.

This is called lateral reading — leaving the source to check what other sources say about it, rather than reading deeper into the source itself. Professional fact-checkers consistently outperform PhD-level experts at evaluating information, and lateral reading is why. They don't try to evaluate a source by studying it. They check what others say about it. It's what I expect you to be doing while reading this book.

A printable reference card for the SIFT framework is available in the companion materials — small enough to keep near your computer or tape to a wall.

Now go back to the claim you found at the beginning of this chapter. Apply SIFT. Write down what you find at each step in your field journal.

Did the ground get more solid, or less?

That question is the core design principle of everything I've been writing. Everything I've told you in these chapters is verifiable. Court filings. Congressional records. Published research. Government procurement documents. If you check my claims and the ground gets less solid — walk away.

Set up a family code word. AI voice cloning can now produce a con-

vincing replica of someone's voice from as little as three seconds of audio. Voice phishing attacks — calls impersonating family members claiming emergencies — surged over 400% in 2024-2025, and deepfake video scams rose 700% in the same period. In one documented case, a Florida woman lost $15,000 after receiving a call from what sounded exactly like her crying daughter claiming she'd been in a car accident. The voice was AI-generated. Agree on a code word with your immediate family or close contacts that you'd use to verify identity over the phone. Something you'd never say in normal conversation. Something not findable in your social media posts. This takes five minutes and it's one of the simplest defenses against the most effective new social engineering attack.

Practice SIFT on two more claims this week. Pick them from different sources — one from a source you trust, one you don't. Apply the full framework. Record the process and findings in your field journal. The point isn't to debunk anything. It's to build the reflex.

Bookmark primary source repositories. These are where you go when you want to verify a claim at the source, not through someone else's summary. Court records: PACER (pacer.uscourts.gov). Congressional records: congress.gov. FOIA reading rooms: fbi.gov/vault, the NSA's declassified documents page. State and local court records through your state judiciary's website. These aren't sources you'll use every day. They're sources you'll be glad you bookmarked when a claim matters.

You now have the tools to see clearly — your data, your communications, your identity, your browser, your information diet. The next question is: how do you maintain all of this without burning out?

Because the number one reason people abandon security practices isn't that they don't care. It's that they're exhausted.

`Summary`

Your mind is as much an attack surface as your devices. Misinformation exploits outrage, urgency, and emotional reactivity — the same psychological triggers used in phishing and social engineering.

`Action Items`

- Apply SIFT to the claim you found at the beginning of this chapter — record each step and your findings in your field journal

- Practice SIFT on two more claims this week, one from a source you trust and one you don't
- Set up a family code word for phone identity verification — something never said in normal conversation and not findable on social media
- Bookmark primary source repositories: PACER (pacer.uscourts.gov), congress.gov, fbi.gov/vault, NSA declassified documents, your state judiciary's court records site

Case Studies & Citations

- **Vosoughi, Roy, & Aral (MIT, 2018)** — Study of 126,000+ stories on Twitter found falsehoods 70% more likely to be retweeted than true stories and reached first 1,500 people six times faster. Published in *Science*. Effect driven by novelty and emotional response (surprise, disgust), not bots.
- **Brady et al. (2024)** — Study published in *Science* across eight studies and two experiments found misinformation sources evoke more outrage than trustworthy sources, and outrage facilitates sharing even when users know content is inaccurate — to signal moral position or group loyalty.
- **Brennan Center / Dataminr** — 160,000 email alerts sent to DC police over two years tracking planned demonstrations, protest organizers, and march movements in real time. Included social media profile of college graduate with fewer than 100 followers who shared an event announcement.
- **AI voice cloning / deepfake surge** — Voice phishing attacks surged over 400% in 2024-2025 (multiple sources including FBI alerts, BlackFog, Pcdn). Deepfake video scams rose 700% in 2025 (ScamWatch HQ, Gen Threat Labs). McAfee 2024 study found 1 in 4 adults experienced an AI voice scam. A Florida woman lost $15,000 to a cloned voice impersonating her daughter (WFLA, 2025).
- **SIFT method** — Developed by Mike Caulfield, digital literacy researcher. Four-step framework: Stop, Investigate the source, Find better coverage, Trace claims to origin. Built on lateral reading — the practice of leaving a source to verify it externally rather than reading deeper into the source itself. Professional fact-checkers outperform PhD-level domain experts using this approach.

Templates, Tools & Artifacts

- **SIFT Method** — Stop → Investigate the source → Find better coverage → Trace claims to origin. Apply to any claim before sharing or acting on it. Record results in field journal.
- Download: SIFT Framework Reference Card
- **Family Code Word Protocol** — Agree on a word or phrase with immediate family/close contacts for phone identity verification. Requirements: never used in normal conversation, not findable in social media posts, shared only in person or via encrypted channel. Use when receiving any unexpected urgent call requesting money or action.
- **Primary Source Repositories** — PACER (pacer.uscourts.gov) for federal court records. Congress.gov for congressional records and legislation. FBI Vault (fbi.gov/vault) for FOIA documents. NSA declassified documents page. Your state judiciary website for state/local court records.
- **Lateral Reading** — Verification technique: instead of reading deeper into a source to evaluate it, leave the source and check what other sources say about it. Search for the claimant, not just the claim.

Key Terms

- **SIFT** — Four-step information verification framework (Stop, Investigate the source, Find better coverage, Trace claims to origin) developed by digital literacy researcher Mike Caulfield.
- **Lateral reading** — The practice of leaving a source to check what other sources say about it, rather than evaluating a source by reading deeper into it. The method that distinguishes professional fact-checkers from domain experts.
- **Voice phishing (vishing)** — Phone-based social engineering using AI-cloned voices to impersonate family members, executives, or officials. Exploits urgency and emotional response. Surged over 400% in 2024-2025.
- **Deepfake** — AI-generated synthetic media (audio, video, or images) designed to convincingly impersonate real people. Consumer-grade tools now produce realistic results from seconds of source audio or a few images.
- **Family code word** — A pre-agreed verification phrase shared only among trusted contacts, used to confirm identity during unexpected phone calls. Effective defense against voice cloning because the AI can only reproduce voice, not knowledge the cloner doesn't have.

Chapter 11

When to Worry and When to Live

I've been writing for five days straight and I can feel the edges of my own thinking getting sloppy, and the thing I need to tell you tonight is that getting sloppy is the biggest risk you face right now. Not surveillance. Not misinformation. Fatigue.

If you've been following these chapters and doing the work, you now know more about digital security, surveillance infrastructure, and information integrity than the vast majority of people around you. You've checked your location history. You've audited your apps. You've built a threat model. You've secured your passwords and enabled two-factor authentication. You've moved at least one conversation to Signal. You've started opt-outs from data brokers. You've seen your browser fingerprint. You've practiced evaluating information at the source.

That's a lot. In less than a week.

And if you're feeling overwhelmed, that's not weakness — it's a documented psychological response. In 2016, researchers at the National Institute of Standards and Technology published a study on what they called security fatigue — the weariness and reluctance people develop toward dealing with computer security. Brian Stanton, Mary Theofanos, and their colleagues interviewed forty typical computer users and found that more than half expressed fatigue unprompted. The participants weren't indifferent to security. They were overwhelmed by it. They described resignation, loss of control, fatalism. The researchers found that this fatigue directly contributed to poor security decisions — not because people stopped caring, but because caring without a sustainable practice became unbearable. They reached a point where every notification felt like a threat, every setting felt inadequate, and the gap between what they knew and what they'd done felt insurmountable. So they stopped.

Don't stop.

Here's how this works sustainably. Not everything you've learned needs to be active all the time. Security is not one state — it's two modes.

If you've seen the show Severance, you know the premise: employees at Lumon Industries undergo a procedure that splits their consciousness. Their work selves — the "innies" — know nothing about their lives outside the office. Their outside selves — the "outies" — know nothing about what happens at work. Two completely separate identities, each operating in its own sealed compartment. Lumon designed it that way because compartmentalization is control. When your selves can't talk to each other, neither one has the full picture. Neither one can act on the whole truth.

The severed floor is what happens when you treat security as a set of disconnected tasks instead of an integrated practice. One version of you audits your apps. Another version checks your data broker listings. A third version manages your passwords. None of them talk to each other. None of them see the whole picture. And eventually, each one burns out independently, because compartmentalized effort is exhausting in a way that integrated habit is not.

What you need is the opposite of severance. You need your security practices to be one continuous identity — some things you do always, some things you activate when the context changes, all of them connected to the same threat model.

There are daily habits. These are things you do every time, without thinking, because they're now part of how you operate. Use your password manager. Communicate sensitive things on Signal. Don't reuse passwords. Don't click links in unexpected messages without checking. These become automatic. They cost almost nothing once they're habits.

Then there are situational activations. These are things you do when your threat level changes — when you're going to a protest, traveling internationally, dealing with a stalker, starting a new job with higher exposure. Reviewing your data broker listings. Tightening your social media privacy settings. Checking your phone for unfamiliar apps. Updating your threat model. You don't do these every day. You do them when the context calls for it.

The distinction matters because it's the difference between a practice you can maintain for years and a state of hypervigilance you'll abandon in a month. Good enough security practiced consistently beats perfect security abandoned after four weeks.

Consolidate. Open your field journal and build a personal security checklist from everything you've done. Not everything you've learned — everything you've actually done.

Your checklist should have three sections.

What you've changed permanently — password manager installed, Signal as default for sensitive conversations, search engine switched, uBlock Origin running. These are your new defaults.

What you maintain on a schedule — data broker opt-outs every three to four months, app permission audit quarterly, HIBP check quarterly, devices updated when prompted. Put these in your calendar. Literally. Make them recurring reminders.

What you activate situationally — threat model review before changes in exposure, burner practices for high-risk contexts, full self-OSINT check if you suspect you're being targeted. These stay in your field journal as reference, not as daily tasks.

Write it out. This document is your proof — to yourself — that you've done the work. A printable checklist with all three sections is available in the companion materials.

In 2019, Hong Kong protesters developed some of the most sophisticated collective security practices any civilian movement has ever produced. They used Telegram with pseudonymous accounts. They paid for transit in cash. They used AirDrop to share maps and updates without internet connections — device to device, bypassing censorship entirely. They wore matching dark clothing to make individual identification harder. They developed hand signals for communicating across crowds. They used mesh networking apps when cell service was disrupted. Group administrators in private channels assumed security roles, purging compromised members and rotating access when someone was arrested.

Despite all of this — despite extraordinary discipline practiced collectively by tens of thousands of people — over 10,200 were arrested. That number comes from Hong Kong government disclosures to lawmakers, covering the twenty months from mid-2019 onward.

The lesson isn't that security practices fail. The lesson is that individual security has a ceiling. The protesters who survived longest, who maintained the most operational freedom, were the ones who practiced security collectively. Their threat models accounted for each other. Their communication practices were shared norms, not individual choices.

Everything you've learned in these chapters is real. It works. And it has a structural limit that no amount of individual discipline can overcome. Your security ceiling is set by the least secure person you communicate with. You can encrypt everything on your end. If the person you're talking to screenshots the conversation and posts it, encryption didn't help.

There's one more chapter in Part 1. It talks about the hardest skill of all — and the one I think matters more than any of the others.

Summary

Security fatigue is the greatest threat to everything you've built in the previous ten chapters. The antidote is integration, not compartmentalization: organizing your practices into daily habits, scheduled maintenance, and situational activations so that security becomes a sustainable identity rather than an exhausting activity. Individual security also has a structural ceiling — your practices are only as strong as the least secure person you communicate with — which is why the next chapter shifts from what you do alone to who you do it with.

Action Items

- Build your personal security checklist in your field journal with three sections: permanent changes, scheduled maintenance, situational activations.
- Set recurring calendar reminders for your scheduled maintenance items (quarterly data broker opt-outs, app permission audits, HIBP checks).
- Review your checklist against the work from Chapters 2–10 to make sure nothing you've done falls through the cracks.

Case Studies & Citations

- **NIST Security Fatigue Study** — Stanton, B., Theofanos, M., Prettyman, S.S., & Furman, S. (2016). "Security Fatigue." *IT Professional*, 18(5), 26–32. Published by IEEE. The foundational research on why overwhelmed users abandon security practices.
- **2019 Hong Kong Protests** — Over 10,200 arrested during 2019–2021 despite sophisticated collective security practices including pseudonymous communications, cash transit, AirDrop distribution, mesh networking, and rotating channel administration. Arrest figures from Hong Kong government disclosures to lawmakers (South China Morning Post, April 2021; Hong Kong Free Press, June 2024).

Templates, Tools & Artifacts

- **Personal Security Checklist Template** — Three-section framework: (1) Permanent changes / new defaults, (2) Scheduled maintenance with calendar frequency, (3) Situational activations with trigger conditions. Build in your field journal.
- Download: Personal Security Checklist

Key Terms

- **Security fatigue** — The weariness and reluctance to deal with security decisions, leading to resignation, risk minimization, and decision avoidance. Identified by NIST researchers as a primary driver of poor security behavior among people who are aware of risks but overwhelmed by the effort of managing them.
- **Daily habits vs. situational activations** — Framework for organizing security practices into two modes: things you do automatically every time (password manager, Signal, no link-clicking) and things you activate when your threat level changes (protest attendance, international travel, targeted harassment). The distinction between sustainable practice and unsustainable hypervigilance.

Chapter 12

The Hardest Skill

The hardest skill I can teach you has nothing to do with technology.

It's this: convincing someone you care about to take their security seriously when they think they have nothing to hide.

I've heard every version of the objection. "I'm not doing anything wrong." "If they want to look at my boring life, let them." "I don't have time for this." "You're being paranoid."

None of these are wrong, exactly. They're just incomplete. The person saying them isn't stupid and they're not naive — they're making a rational calculation based on incomplete information. They haven't seen what you've seen over the last week. They haven't checked their location history, or found their home address on a people-search site, or watched their browser fingerprint get read by a dozen trackers in real time. They're assessing risk based on what they know. You now know more.

The mistake is leading with fear. Research on security behavior — particularly a 2018 longitudinal study by Mwagwabi, McGill, and Dixon on fear appeals and password compliance — found that persuasive communication improved security behavior in the short term, but the effects on compliance intentions didn't last. More striking: neither perceived vulnerability to an attack nor perceived severity of an attack predicted sustained compliance. What predicted it was self-efficacy — the person's belief that they could actually do something effective — and response efficacy — their belief that the recommended action would actually work. Fear gets people to act once. Believing they can act, and that acting matters, gets them to keep going.

This is why most security advice fails. It makes people feel helpless, so they stop listening.

What works is framing security as care. Not "the government is watching" — but "I want to protect our conversations." Not "you're exposed" —

but "I found something that helps, want me to show you?" Not a lecture. A gift.

The behavioral research on adoption reinforces this. The MINDSPACE framework — developed in 2010 by Paul Dolan and colleagues for the UK Cabinet Office, and the foundation for the government's Behavioural Insights Team — identifies nine factors that shape behavior. Three are especially relevant here. The messenger matters more than the message: people adopt practices from people they trust, not from experts or institutions. Social norms drive behavior more than logic: knowing that someone they respect already uses Signal is more persuasive than any technical argument. And defaults shape action: if Signal is where the group chat lives, people use Signal.

Here's what works in practice.

Start with one person. Not a group — one person you're close to. Someone who trusts you. Ask them to install Signal with you. Do it together — in person or on a call, not by text. Walk through the setup. Make it a shared activity, not an assignment.

Don't explain the surveillance pipeline. Don't mention metadata. Just say: "This is a better messaging app. The conversations are private, the group chats are cleaner, and it doesn't show ads. Can we try it?"

If they push back, you have real stories now. Not abstract threats — specific cases from this book. A Catholic priest whose anonymized location data from a dating app was correlated with his church and his home until he was identifiable — and whose career was destroyed when The Pillar published the story. A cyclist in Gainesville who spent thousands of dollars on a lawyer because his location data placed him near a burglary he had nothing to do with. A woman identified through a chain that started with a reused username on a shopping site — one account linked to another linked to another until her real identity surfaced from behind layers she thought were separate. These are real people whose lives changed because the ordinary digital systems around them worked exactly as designed.

Use whichever story matches what the person cares about. Privacy? The Burrill case. Wrongful suspicion? McCoy. Identity exposure? Blumenthal. You're not scaremongering. You're translating what you've learned into something relevant to them.

Once Signal is installed, move one existing group chat there. A family chat. A friend group. A book club. The content of the chat doesn't have to

be sensitive — the point is normalizing a more secure default. Once people are using Signal for the mundane stuff, they'll use it when it matters.

Then teach one thing. Just one. Not everything you know — one concept, one skill, one action from this book. Maybe it's checking haveibeenpwned.com. Maybe it's the password manager. Maybe it's the SIFT method from Chapter 10. Pick the thing you think will land and share it the way you would share a useful tool you found, not the way you'd deliver a warning or a lecture.

Install Signal with one person who doesn't have it yet. Do it together. In person or on a call.

Move one existing group chat to Signal. Pick the one with the most momentum — the chat people actually respond in.

Teach one concept from this book to someone who hasn't read it. Record in your field journal: who you talked to, what you shared, what worked, what resistance you encountered.

If you've done everything in these chapters, you've changed how you move through the world. You see the infrastructure. You've secured yourself against the most common vectors. You have a threat model, a field journal, and a maintenance schedule. You know how to evaluate information at the source. And you have at least one person you've brought along.

That's Level 1. Seeing clearly.

In The Hunger Games, there's a moment when Katniss raises three fingers in a silent salute to the cameras. She's not giving a speech. She's not issuing orders. She's making a gesture that says: I see you. I'm with you. It costs her nothing but attention — and it becomes the most dangerous thing in Panem because other people start doing it too. Not because they were told to. Because they recognized something in it.

The three-finger salute isn't a token. It's not a password, or a badge, or a membership card. It can't be counterfeited because it isn't a thing — it's a recognition. The districts don't exchange credentials. They recognize shared experience. You know the salute because you lived through what made it necessary.

That's how this works too.

I'm not going to give you a key, or a code, or a secret phrase to unlock what comes next. There's no gate between Level 1 and Level 2. You can read the next chapter right now if you want. But the content of Level 2 as-

sumes you've done the work — not because I'm testing you, but because the skills build on each other. If you haven't built a threat model, the group security practices in Level 2 won't make sense. If you haven't had the conversation from this chapter — the one where you sit with another person and help them install Signal, or teach them one concept, or share one story that makes abstract risk feel personal — then Level 2 will be instructions for a game you're not yet playing.

The threshold isn't something I give you. It's something you already have if you've done the work. Check:

You have a field journal with your threat model, your security checklist, and your maintenance schedule.

You have Signal installed and at least one conversation happening there.

You've taught at least one person at least one thing from this book.

You recorded what worked and what didn't.

If those are true, you're ready. You have the required skills for what comes next.

The narrow path isn't walked by individuals. Every scenario I've studied where things hold together — where communities maintain trust, where institutions face accountability, where the machinery of surveillance breaks down — those scenarios feature well-secured people who found each other, built trust, and organized.

They built a network.

Summary

The shift from individual security to social security is the most important step. Fear-based messaging about security produces short-term compliance. The bridge from individual practice to group practice is the key to accessing Level 2.

Action Items

- Install Signal with one person who doesn't have it yet. Do it together, in person or on a call.
- Move one existing group chat to Signal — pick the one with the most activity.
- Teach one concept from this book to someone who hasn't read it. Record in your field journal: who, what, how it landed, what resistance you encountered.
- Complete the self-assessment: field journal with threat model and security checklist, Signal installed with at least one active conversation, at least one teaching interaction documented.

Case Studies & Citations

- **Jeffrey Burrill** — Catholic priest identified through anonymized Grindr location data purchased from a commercial data broker. Reported by The Pillar (July 2021). Referenced as persuasion example for privacy-focused conversations.
- **Zachary McCoy** — Cyclist in Gainesville, FL, identified by Google geofence warrant as suspect in a nearby burglary. Spent thousands on legal defense before being cleared. Reported by NBC News (March 2020). Referenced as persuasion example for wrongful-suspicion conversations.
- **Identity chain exposure (Blumenthal pattern)** — Individual identified through a chain of reused usernames across platforms, linking pseudonymous accounts to real identity. Referenced as persuasion example for identity-exposure conversations.
- **Fear appeals and security compliance** — Mwagwabi, F., McGill, T., & Dixon, M. (2018). "Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines." *Communications of the Association for Information Systems*, 42(1). Found self-efficacy and response efficacy predict sustained compliance; perceived vulnerability and severity do not.
- **MINDSPACE framework** — Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). "MINDSPACE: Influencing behaviour through public policy." UK Cabinet Office / Institute for Government. Nine behavioral influences: Messenger, Incentives, Norms, Defaults, Salience, Priming, Affect, Commitments, Ego.
- **Three-finger salute in real protest** — The Hunger Games gesture was adopted by Thai pro-democracy protesters (2014, 2020–2021) as a symbol of resistance, demonstrating how fictional recognition signals cross into lived political practice.

Templates, Tools & Artifacts

- **Persuasion script framework** — Match the case study to the listener's concern: privacy → Burrill, wrongful suspicion → McCoy, identity exposure → Blumenthal pattern. Lead with care ("I found something that helps"), not fear ("you're being watched").
- **Signal migration checklist** — (1) Install together, in person or on call. (2) Move one active group chat. (3) Make Signal the default for sensitive conversations. (4) The mundane conversations normalize the tool.
- **Level 1 self-assessment** — Four checks: field journal with threat model and security checklist; Signal installed with at least one active conversation; at least one teaching interaction completed and documented; maintenance schedule set with calendar reminders.

Key Terms

- **Security fatigue** — Covered in Chapter 11. The exhaustion that leads people to abandon security practices. Relevant here because fear-based persuasion triggers the same fatigue in others.
- **Self-efficacy (in security adoption)** — A person's belief that they can effectively perform the recommended security behavior. Research shows this predicts sustained compliance more strongly than perceived threat severity.
- **Response efficacy** — The belief that the recommended action will actually work to reduce the threat. Together with self-efficacy, the strongest predictor of long-term security behavior change.
- **MINDSPACE** — A behavioral influence framework identifying nine factors that shape decision-making: Messenger, Incentives, Norms, Defaults, Salience, Prim-

ing, Affect, Commitments, and Ego. Developed by Dolan et al. (2010) for the UK Cabinet Office.

- **Threshold (as used in this book)** — Not a gate, badge, or token. A self-assessed readiness based on demonstrated competency. You cross the threshold by having done the work, not by receiving permission.

Level 2

Find Each Other

Chapter 13

The First Conversation

Everything I've published so far was designed for a single person sitting alone with a phone, learning to see the infrastructure they live inside. And it worked. If you've done the work — checked your location history, audited your permissions, locked down your browser, learned to verify before you share — you are materially harder to surveil, to manipulate, and to isolate than you were two weeks ago.

But the narrow path isn't walked by individuals.

I need to tell you something about what I found in the projections that I've been holding back — not because it's secret, but because it wouldn't have meant anything until now. I told you the model ran millions of scenario branches. What I didn't tell you is how it sorted them. The variable that best predicted whether a scenario branch held together — better than economic conditions, better than policy, better than the specific threat — was the density of trusted relationships in a population. Not social media connections. Not organizational memberships. Relationships where people had done something difficult together and come out the other side trusting each other more.

The scenarios where things fell apart weren't the ones with the worst governments or the most surveillance. They were the ones where people were alone. Where the infrastructure existed to connect them but the relationships didn't. Where everyone could see the problem and no one had anyone to call.

I've been building your individual capability because that's where the path starts. But individual capability has a ceiling, and you've reached it. Everything from here requires another person.

That probably sounds simple but it isn't.

The social is much harder than the technical. I know this because I'm

living it. I'm an evaluation researcher — I'm trained to probe systems, not to build trust with strangers. Everything that comes next, I've had to learn in real time, like the Industrial Areas Foundation's relational meeting model, SNCC's field secretary approach, decades of documented practice from people who understood something I'm only now understanding — that relationships precede organizing. Always. In every tradition. Everywhere.

The IAF calls it a "one-to-one." In *Roots for Radicals*, Ed Chambers — Saul Alinsky's successor as executive director of the IAF — devoted an entire chapter to the relational meeting as the foundation of organizing. The concept sounds grandiose until you realize what it actually is: a structured conversation where one person listens to another person without interrupting, solving, or relating. Just listens. Most people have never experienced this. Most people have never been asked "what do you care about?" and then given uninterrupted time to answer.

That's your first challenge. And it's with the person you already have.

If you completed the chapters in Level 1, you brought someone along. You installed Signal with them, or taught them something, or moved a group chat. You have at least one person who knows you've been doing this work. That person is your partner for what comes next.

This isn't a planning session. It's not a strategy meeting. It's a conversation with a specific structure, and the structure matters because it does something most conversations don't — it creates space for someone to be heard.

Here's what you do.

Find 45 minutes. In person if you can — a kitchen table, a park bench, a car in a parking lot. If you can't meet in person, a phone or video call works. Not text. You need to hear each other's voices.

Each of you gets 15 minutes of uninterrupted time. The person speaking answers three questions — not all at once, but as a flow: Why do you care about this? What are you afraid of? What do you want to protect in your community?

The person listening does one thing: listens. No responding. No "me too." No solving the problem they just described. No reaching for your phone. Fifteen minutes of your full attention on another human being. Then you switch.

After both of you have spoken, spend 10 to 15 minutes in open conver-

sation about what you heard. Not what you agreed with — what you *heard*. What surprised you. What you didn't expect.

Then write what you learned in your field journal. Not a transcript. An impression. What moved the other person. What moved you. Where your concerns overlap. Where they diverge.

I want to be direct about why this works.

The organizing traditions I've studied — IAF, SNCC, the Highlander Center, farmworker movements, church-based organizing across every denomination — they disagree about almost everything. Strategy, tactics, structure, ideology. But they converge on one finding so consistent it might as well be a law of organizing physics: the relationship comes first. Before the plan. Before the platform. Before the shared threat model. Before anything.

In Frank Herbert's *Dune*, when Stilgar first meets Paul Atreides, he doesn't ask what Paul can do for the Fremen cause. He doesn't pitch a strategy. He assesses. Who is this person? Can I trust them? What do they bring? The Fremen had survived centuries of Harkonnen occupation not because they had superior weapons or a master plan, but because they had a culture of testing before trust — of knowing who someone was before asking them to act.

That's fiction. Here's reality.

Charles Sherrod and Cordell Reagon — SNCC field secretaries — arrived in Albany, Georgia in the fall of 1961 to organize voter registration. They didn't hold a rally. They didn't distribute flyers. They attended church services. They sat on porches. They listened. Charles Payne's *I've Got the Light of Freedom* documents this same approach as practiced across SNCC's organizing projects — he calls the chapter on organizers and their methods "Slow and Respectful Work." The most effective organizing tool these field secretaries had wasn't a speech or a strategy. It was a conversation.

They didn't start by asking people to do something. They started by understanding who people were.

That's what you're doing today. Not building a plan. Not recruiting. Understanding who your partner is — what they care about, what they're afraid of, what they want to protect. The plan comes later. The understanding comes first.

I should be honest about something. Writing these chapters has changed me in ways I wasn't prepared for. I started this as an operational decision — I found something in a model, and the responsible thing to do was publish it. It was rational. Impersonal, almost. I mapped the path, I started sharing the map.

But someone is reading this. You're reading this. And that changes things I didn't expect it to change. I'm not writing into a void anymore. There's a person at the other end of this — someone who checked their location history and sat with what they saw, someone who spent an afternoon opting out of data brokers, someone who taught a friend to use Signal. I don't know who you are. But I know you did the work, because you're still here. We walked together.

Every scenario I've studied where things hold together requires groups, and every group that survives starts with a single honest conversation between two people. Not a pitch. Not a plan. A conversation where someone says "I'm worried about this" and someone else says "me too."

If these chapters become something — if they reach beyond me and beyond you — it's because people like you decided to act. I can map the path. I can't walk it for you. And increasingly, I can't walk it alone either.

After your conversation, sit with it for a day. Don't rush to the next chapter. Let the conversation settle. You'll know things about your partner you didn't know before, and they'll know things about you. That's the foundation. Everything we build from here sits on top of it.

The next chapter is about what changes now that your security isn't just yours anymore. Your threat model was individual. Now it's shared. That's a different kind of problem — and a different kind of strength.

Summary

Level 2 begins by acknowledging that individual capability has a ceiling — the density of trusted relationships, not individual preparedness, is what determines whether communities hold together. The IAF's one-to-one relational meeting is the first tool: a structured conversation where two people listen to each other without solving, relating, or interrupting.

Action Items

- Conduct a one-to-one relational meeting with your Level 1 partner. 45 minutes: 15 minutes each of uninterrupted speaking (Why do you care? What are you afraid of? What do you want to protect?), then 10–15 minutes discussing what you heard.
- In person if possible. Phone or video call if not. Not text — you need to hear each other's voices.
- Record in your field journal: not a transcript, but an impression. What moved them. What moved you. Where your concerns overlap. Where they diverge.
- Sit with it for a day before moving to the next chapter.

Case Studies & Citations

- **SNCC field secretaries in Albany, Georgia** — Charles Sherrod and Cordell Reagon arrived in Albany in fall 1961 as SNCC field secretaries to organize voter registration. They didn't hold rallies or distribute flyers — they attended church services, sat on porches, and listened. Their approach exemplified the organizing principle that relationships precede action. Sources: SNCC Digital Gateway; New Georgia Encyclopedia; Charles Payne, *I've Got the Light of Freedom: The Organizing Tradition and the Mississippi Freedom Struggle* (University of California Press, 1995/2007), Chapter 8: "Slow and Respectful Work" — documents SNCC's broader organizing philosophy of patient, relational groundwork.
- **IAF one-to-one (relational meeting)** — Edward T. Chambers, *Roots for Radicals: Organizing for Power, Action, and Justice* (Continuum, 2003), Chapter 2: "The Relational Meeting." Chambers, Saul Alinsky's successor as IAF executive director (1972–2009), established the one-to-one as a foundational organizing practice. The IAF model emphasizes listening, understanding values and self-interest, and building relational power before taking action.
- **Convergence across organizing traditions** — The principle that "relationships precede organizing" appears independently across IAF, SNCC, the Highlander Center, farmworker organizing (Cesar Chavez/Dolores Huerta via Fred Ross's house meetings), and church-based organizing traditions. Despite disagreements on strategy and ideology, this convergence is one of the most robust findings in the organizing literature.

Templates, Tools & Artifacts

- **One-to-one relational meeting script** — (1) Find 45 minutes, in person preferred. (2) Each person gets 15 minutes of uninterrupted speaking time. Three guiding questions: Why do you care? What are you afraid of? What do you want to protect in your community? (3) Listener's only job: listen. No responding, no "me too," no solving. (4) After both have spoken, 10–15 minutes of open conversation about what you heard — not what you agreed with. (5) Each person writes an impression in their field journal.
- **Field journal prompt for this chapter** — What moved your partner? What moved you? Where do your concerns overlap? Where do they diverge? What surprised you about listening for 15 uninterrupted minutes?

Key Terms

- **One-to-one (relational meeting)** — A structured conversation from the IAF organizing tradition where two people take turns listening to each other without interruption. The purpose is understanding — what someone cares about, what they're afraid of, what they want to protect — not agreement or planning.

- **Relational power** — The capacity that comes from trusted relationships between people, as distinct from positional power (authority from a role) or institutional power (authority from an organization). In the IAF framework, relational power is built through one-to-ones and is the foundation of all effective organizing.
- **Field secretary** — SNCC's term for organizers sent into communities to build relationships and support local leadership. Field secretaries like Charles Sherrod practiced "slow and respectful work" — listening before organizing, understanding before acting.

Chapter 14

Security Is a Conversation Now

Your threat model was yours. Now it includes another person.

That changes things. When your security was individual, the decisions were yours alone — which browser, which password manager, whether to opt out of data brokers. You could make choices at your own speed, at your own risk tolerance, on your own schedule. That's over. From here, the things you protect include someone else's identity, someone else's concerns, someone else's willingness to be part of this. Your security decisions are now negotiations.

I want to name a paradox before we go further, because you're probably already living it.

You and your partner found each other through compromised channels. Maybe it was a text message. Maybe a conversation at a coffee shop. Maybe Facebook, Discord, or a group chat on a platform that logs everything. That's fine. I'm not going to pretend you should have established perfect operational security before your first conversation — you didn't have the infrastructure, and you didn't have the trust. You can't coordinate a move to secure channels on the insecure channel you're trying to leave. That's the bootstrapping paradox, and every group in history has faced some version of it.

The EFF's harm reduction philosophy — the same one that guides their Surveillance Self-Defense project — applies here: no one locks everything down in one day. You don't go from texting on iMessage to running Tails on a burner laptop overnight. You establish a baseline, you commit to it together, and you build from there. The floor rises over time. But it has to start somewhere, and it starts with an honest conversation about where each of you actually is.

Here's what's different about shared security. When you were alone,

a mistake cost you. Now a mistake can cost your partner. The economist Jack Hirshleifer described this as the weakest-link model in a 1983 paper on public goods: in systems where the outcome depends on the least contribution, the whole system is only as strong as its most vulnerable point. Security researchers have since applied this widely — airport security, network firewalls, epidemic response — and it maps precisely to group security. Your pair's security isn't the average of your individual practices. It's defined by whichever one of you is less secure.

It's a coordination problem. And the solution to a coordination problems is always the same: you talk about it.

In *The Matrix*, Neo and Trinity survive because their trust isn't abstract — it's operational. They don't just believe in each other. They know each other's capabilities, cover each other's vulnerabilities, and communicate through channels they've verified. When Trinity tells Neo to trust her, she's not asking for faith. She's asking him to rely on the security practices they've built together. Their relationship isn't separate from their operational security — it *is* their operational security. The love story is also a shared threat model.

That's closer to reality than most people realize. The strongest security posture two people can have isn't two individuals with perfect practices. It's two people who know exactly where the other is strong and where they're exposed, and who have agreed — out loud, explicitly — on how to protect each other.

So here's your challenge. Sit down with your partner — in person if you can, on a Signal call if you can't — and build a shared threat model. You both did individual threat models in Level 1. Pull them out. Now do this together.

Share your threat models with each other. Not the whole document — the relevant parts. What are you each most concerned about? Where do your risks overlap? Where do they diverge? One of you might be worried about an ex with a tracking habit. The other might be worried about an employer who monitors social media. Both are real. Both affect the pair.

Identify your shared floor. This is the minimum set of practices you both commit to. Not aspirational — real. Things you will actually do, starting today.

A starting floor that makes sense for most pairs:

Communication happens on Signal. Not some of it — all of it. If you're not both on Signal yet, that's the first thing you fix. Disappearing mes-

sages on, set to one week for general conversation. This isn't paranoia. It's hygiene — the same reason you don't leave your medical records on the kitchen table when guests come over.

Device security baseline: alphanumeric passcode (not four digits, not a pattern), operating system current, notification previews off on your lock screen. You covered all of this in Level 1. Now you verify that your partner has too.

Information boundaries: what about your partnership stays private? Who knows you're doing this? What would you tell someone who asked? Having an answer to these questions before someone asks is the difference between a considered response and a panicked one.

Write the floor down. Both of you keep a copy. Not because you'll forget — because writing it makes it real. It transforms "we should probably use Signal" into "we agreed to use Signal, and here's the document that says so."

I want to plant something here that I'll come back to in a later chapter.

Security, at the individual level, is a set of practices. You do them or you don't. But security at the pair level — and eventually at the group level — is something else. It's an act of care. When you configure disappearing messages, you're not protecting yourself. You're protecting your partner. When you use a strong passcode, you're making a decision about someone else's exposure, not just your own. When you have the awkward conversation about "hey, your notification previews are showing our messages on your lock screen," you're doing something that's uncomfortable because you care about the person on the other end of that conversation.

Security as care. Remember that phrase.

There's a case I need to tell you about, because it illustrates what happens when a group doesn't have this conversation.

In 2020, the FBI paid a convicted felon named Michael Windecker to infiltrate racial justice organizing in Denver during the protests following the killing of George Floyd. The Intercept's Trevor Aaronson reported the story in 2023, drawing on internal FBI records and undercover recordings. Windecker drove a silver hearse to protests, carried guns, and worked his way into activists' inner circles. He was paid at least $20,000 by the FBI over that summer. He accused real activists of being informants — a tactic directly out of the COINTELPRO playbook documented by the Church

Committee in 1975. He tried to entrap activists in violent plots. He pushed demonstrations toward destruction.

What made the infiltration effective wasn't just Windecker's tactics — it was the absence of shared security practices in the groups he entered. No one had sat down together and agreed on a security floor. There was no conversation about what information stayed internal. No agreement on communication channels. No protocol for when someone new showed up with unusual resources and extreme enthusiasm — which is exactly what Windecker brought. Signal existed. Encrypted channels were available. But no one had done together what you're about to do: have the conversation, write the floor, commit to it as a pair.

I don't tell you this to make you paranoid about the people around you. I tell you because the fix is concrete and you're about to do it. The groups that survive aren't the ones with the best tools. They're the ones who agree to use them.

After you've built your shared floor, test it. Send each other a Signal message with disappearing messages on. Verify each other's Safety Numbers — in person, scanning the QR code, not just comparing numbers on a screen. Check that notification previews are off on both phones. These aren't trust exercises. They're calibration. You're making sure the floor you agreed to is actually under your feet.

Then write in your field journal what this conversation was like. Not the technical details — the experience. Was it awkward? Was it easier than you expected? What did you learn about your partner's risk tolerance that surprised you? This is the beginning of something that shows up in every successful group formation I've studied: the ongoing conversation about how you protect each other. It's not a one-time setup. It's a practice.

The next chapter expands the frame. You and your partner have trust and shared security. The question now is: who else?

Summary

Individual security becomes shared security when a second person is involved. The weakest-link principle means your pair's security is defined by whichever partner is less secure — not by the average. The fix is a shared security floor: minimum practices both partners commit to, written down, tested together. Security at the pair

level is an act of care, not just a set of practices.

Action Items

- Pull out your individual threat models from Level 1. Share the relevant parts with your partner.
- Identify your shared floor — the minimum security practices you both commit to starting today. Suggested starting floor: all communication on Signal with disappearing messages (one week), alphanumeric passcode, current OS, notification previews off, information boundaries agreed.
- Write the floor down. Both partners keep a copy.
- Test the floor: send a Signal message with disappearing messages on, verify Safety Numbers in person (QR code scan), confirm notification previews off on both phones.
- Record in your field journal: what the conversation was like, what surprised you about your partner's risk tolerance, what was awkward, what was easier than expected.

Case Studies & Citations

- **Denver FBI infiltration (2020)** — Michael Adam Windecker II, a convicted felon paid at least $20,000 by the FBI, infiltrated racial justice organizing in Denver during the summer of 2020 George Floyd protests. Windecker used COINTELPRO-style tactics including accusing real activists of being informants and attempting to entrap activists in violent plots. Reported by Trevor Aaronson, The Intercept (February 2023); documented in the "Alphabet Boys" podcast (iHeartPodcasts/Western Sound, 2023). The case illustrates what happens when groups lack shared security agreements — the absence was social, not technological.
- **Hirshleifer weakest-link model** — Hirshleifer, J. (1983). "From weakest-link to best-shot: The voluntary provision of public goods." *Public Choice*, 41(3), 371–386. Applied to security: the system's protection level is determined by its least-secure component, not the average.
- **EFF harm reduction philosophy** — The Electronic Frontier Foundation's Surveillance Self-Defense project uses a harm reduction framework: incremental improvement over time rather than demanding perfect security immediately. Applied here to the bootstrapping paradox of establishing secure channels.
- **COINTELPRO and the Church Committee** — The FBI's domestic surveillance program (1956–1971) and its exposure by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee, 1975). Tactics including snitch-jacketing (accusing real leaders of being informants) documented in the Church Committee's final report.

Templates, Tools & Artifacts

- **Shared security floor template** — (1) Communication: all conversations on Signal, disappearing messages set to one week. (2) Device baseline: alphanumeric passcode, current OS, notification previews off. (3) Information boundaries: who knows about the partnership, what stays private, agreed response to questions. (4) Verification: Safety Numbers confirmed in person via QR code scan.
- **Shared threat model worksheet** — Compare individual threat models side by side. Identify: overlapping concerns, divergent risks, the least-secure practices in the pair, and specific commitments to raise the floor.

`Key Terms`

- **Bootstrapping paradox** — The challenge of coordinating a move to secure channels while still on the insecure channel you're trying to leave. Every group faces this. The solution is accepting imperfect starting conditions and establishing a floor that rises over time.
- **Security floor** — The minimum set of security practices a pair or group commits to. Not aspirational — actual. Written down and verified. The floor rises over time but must start somewhere concrete.
- **Weakest-link (in security)** — The principle that a group's security is defined by its least-secure member, not the average. From Hirshleifer's 1983 public goods model, widely applied to security contexts.
- **Security as care** — The reframing of security practices from individual discipline to relational commitment. Configuring disappearing messages protects your partner, not just you. Introduced here, developed across Level 2.
- **Safety Numbers (Signal)** — A verification feature in Signal that confirms you're communicating with the intended person and not a man-in-the-middle. Best verified in person by scanning each other's QR codes.

Chapter 15

How to See Your Neighborhood

You have a partner. You have a shared floor. Now the question becomes: who else?

I want to be specific about that question, because the obvious answer is the wrong one. The obvious answer is: find people who agree with you. Find people who share your politics, your worldview, your analysis of what's happening. Build a group of like-minded people.

Every case I've studied says this fails.

It took me a while to accept this, because it's counterintuitive. Groups built around political agreement feel stronger in the early stages — there's less friction, less negotiation, less discomfort. But the documented pattern is consistent: groups anchored in shared ideology fragment under pressure. When the external situation changes — when priorities shift, when new information contradicts the shared analysis, when a member's views evolve — ideological groups either enforce conformity or splinter. Neither outcome produces the kind of resilient network the path requires.

The groups that held together were anchored in something else: shared place.

This is not a new finding. When Indivisible published their organizing guide in December 2016, the most successful element wasn't the congressional-pressure strategy — it was the interactive map. By mid-2017, roughly 6,000 groups had registered on it, self-forming around congressional districts. Theda Skocpol's research team at Harvard studied these groups and found that the ones that survived went beyond the guide's original model entirely — they pivoted to local elections, school boards, municipal governance. The bridge to sustained action wasn't ideology. It was geography.

When Bed-Stuy Strong organized COVID mutual aid in Brooklyn's Bedford-Stuyvesant neighborhood in March 2020, they split the area into four delivery quadrants. Something unexpected happened. Volunteers started iden-

tifying with their quadrant — the bounded geography generated shared identity, not the other way around. Within months, the network had reached every block in a neighborhood of 250,000 people.

When Belarusians formed resistance networks after the 2020 election, the organizing unit wasn't a political faction. It was the apartment courtyard. The people who lived close enough to look out the same window.

Your neighborhood is full of people who disagree about almost everything but care about the thing outside their window. That's your constituency.

In *Alice in Wonderland*, Alice falls into a world that looks nothing like the one she left. Everything is strange — the scale is wrong, the rules don't apply, the inhabitants operate by logic she doesn't understand. But Alice does something remarkable: she maps it. She moves through Wonderland not by mastering it but by paying attention. She notes who lives where, what matters to them, what makes them dangerous, and what makes them reachable. She builds an operational understanding of a world she didn't choose and can't control.

That's what you're doing this week. You're mapping your own neighborhood — and discovering, like Alice, that it's stranger and more complex than you thought.

Here's what you and your partner do. You map your local landscape. Not the political landscape — the human one.

People you already know. Each of you lists at least five people in your life who've expressed concern about something local. Water quality. School funding. Road safety. Healthcare access. The cost of living. Traffic. The development going up on the corner. The park that's falling apart. Not people who share your politics — people who care about something. You've been listening for this without knowing you were listening for it. Now write it down.

Places where people gather. Where do people in your area actually see each other face-to-face? Churches, community centers, diners, parks, libraries, veteran's posts, barbershops, the bleachers at Friday night games, the parking lot after school pickup. These places matter because they're where relationships already exist — relationships you can build on rather than building from scratch.

What's already happening. Is there a neighborhood association? A mu-

tual aid group? A PTA? A community garden? A civic group? A volunteer fire department? An informal group of parents who coordinate snow days? You're not joining anything yet. You're mapping what exists. Because the cases I've studied showed something else that surprised me: the most effective new groups didn't start from zero. They connected to or grew out of things that were already there.

Map at least ten potential people between you. You won't approach any of them yet — that's the next chapter. Right now, you're doing reconnaissance.

There's a concept from sociology that's worth knowing here, because you'll see it operating in your own map. Mark Granovetter called it "the strength of weak ties" in a 1973 paper that became one of the most cited in the field. The people most likely to bridge you to new networks aren't your close friends — they're the acquaintances you see at the grocery store, the person you chat with at school pickup, the neighbor you wave to but have never had a real conversation with. Close friends tend to know the same people you know. Acquaintances connect you to entirely different networks.

When you're looking at your map, pay attention to the weak ties. The person you sort of know from the community garden. The parent you've exchanged exactly three sentences with at every soccer game for two years. The guy at the coffee shop who always has an opinion about the city council. These people are bridges. They connect your world to worlds you can't see yet.

Write your map in your field journal. Keep it analog — pen and paper, not a shared Google Doc. Not because Google is going to raid your network map. Because you're building a habit of keeping sensitive information off platforms you don't control, and the list of people you might approach about forming a civic group is sensitive information. It's the kind of thing that's perfectly legal and entirely your business and also the kind of thing you don't need indexed and searchable.

Your partner makes their own map. Then you compare. Where do they overlap — the people you both know? Where do they diverge — the networks only one of you can reach? The combined map is larger than either individual map, and the places where your networks don't overlap are the most interesting. Those are the bridges to communities you wouldn't reach

alone.

Sit with the map for a day. Look at the names. Think about who on that list has said something — even once, even in passing — that suggested they were ready for something more than complaining. That person is a candidate. Not a target. A person you might have a real conversation with.

The next chapter is about that conversation.

Summary

Geographic anchoring — organizing around shared place rather than shared ideology — is the strongest predictor of group resilience. Groups built on political agreement fragment under pressure; groups built on proximity and shared local concerns persist. This chapter maps the human landscape around you: people who care about local issues, places where people gather, and existing organizations or informal networks.

Action Items

- Each partner independently lists at least five people who've expressed concern about something local — not political alignment, local concern.
- Map places where people in your area gather face-to-face: churches, community centers, parks, diners, school parking lots, barbershops, bleachers.
- Identify what's already happening: neighborhood associations, mutual aid groups, PTAs, community gardens, informal coordination networks.
- Combine maps with your partner. Identify overlaps and — more importantly — divergences where only one of you has access.
- Write the map in your field journal. Analog, not digital. Keep sensitive information off platforms you don't control.
- Sit with it for a day. Note who on the list has signaled readiness for more than complaining.

Case Studies & Citations

- **Indivisible (2016–present)** — Published an organizing guide in December 2016. By mid-2017, roughly 6,000 groups had registered on their interactive map, self-forming around congressional districts. Theda Skocpol's research team at Harvard (Gose & Skocpol, "Resist, Persist, and Transform," 2019) found that surviving groups pivoted to local elections, school boards, and municipal governance — geography, not ideology, sustained them. Further analysis in Skocpol & Tervo, "Resistance Disconnect," *The American Prospect* (February 2021).
- **Bed-Stuy Strong (2020–present)** — Mutual aid network founded in Brooklyn's Bedford-Stuyvesant neighborhood in March 2020. Split the area into four delivery quadrants for COVID grocery delivery. Supported 28,000 people, raised $1.2 million in grassroots donations. Volunteers developed quadrant-based identity, demonstrating that bounded geography generates shared identity. Sources: Beeck Center for Social Impact & Innovation (Georgetown, 2022); Vice/Motherboard (2020); bedstuystrong.com.
- **Belarus courtyard networks (2020)** — Following the disputed August 2020 presidential election, Belarusians organized resistance through apartment courtyard

networks — neighbors who shared physical proximity rather than political affiliation. The courtyard became the basic unit of distributed protest coordination.
- **Mark Granovetter, "The Strength of Weak Ties"** — Granovetter, M. (1973). "The Strength of Weak Ties." *American Journal of Sociology*, 78(6), 1360–1380. Acquaintances bridge separate social networks more effectively than close friends, who tend to share overlapping connections. Applied here to neighborhood mapping: weak ties are the most valuable bridges to communities you can't currently reach.

Templates, Tools & Artifacts

- **Neighborhood mapping template** — Three categories: (1) People who care about local issues (minimum five per partner). (2) Places where people gather face-to-face. (3) Existing organizations or informal networks. Map individually, then combine. Mark overlaps and unique access points.
- **Weak-tie identification prompt** — For each person on your map, note: How do you know them? How often do you interact? Who do they know that you don't? The people you interact with least frequently but most consistently are likely your strongest bridges.

Key Terms

- **Geographic anchoring** — Organizing around shared place rather than shared ideology. Documented as the strongest predictor of group resilience across Indivisible, mutual aid networks, and international resistance movements.
- **Weak ties** — Acquaintance-level connections that bridge separate social networks. From Granovetter (1973). In organizing, weak ties are more valuable than strong ties for expanding reach because they connect to communities outside your existing circle.
- **Constituency (as used here)** — Not a political grouping — the people who share your physical space and care about what's happening in it, regardless of political alignment.

Chapter 16

The Approach

You've mapped your neighborhood. You know who might be ready. And you haven't talked to any of them yet.

I know. This part is terrifying.

I want to name what's happening, because the fear you're feeling is specific and it deserves to be understood — not just pushed through. You're about to do something that has no undo button. Once you say something to someone, you can't unsay it. If it goes badly — if they think you're strange, if they pull away, if they tell someone else — you can't retrieve the words. Every other skill in this curriculum has a retry. You can reset a password. You can redo a threat model. You can't un-have a conversation.

That's why this is the hardest step in the entire game. Not the most technically complex. The most human.

And it's the step that no existing resource teaches well. I looked. I went through every major organizing tradition, every mutual aid manual, every community security guide published in the last fifty years. They all start after this moment. They assume you've already found your people. The approach — the moment you go from thinking about this to saying something to another human being — is the gap in the literature. It's the gap in every guide I've ever read. And it's the thing I've come to believe is the single highest point of failure across every scenario I can construct: not the lack of skills, not the lack of platforms, not the lack of information. The failure to have the first conversation.

So I'm not going to give you a script.

Scripts are for cold calls. This isn't a cold call. You already know these people — or at least you've noticed them. They're on your network map from last entry. They're the neighbor who mentioned the water quality at the mailbox. The coworker who said something under her breath about

school funding. The person at your place of worship who organized the food drive and looked tired afterward. They're not strangers. They're people you've been paying attention to.

What I can give you are patterns. Not steps to follow — observations about what makes the first real conversation work, drawn from every organizing tradition I've studied. They converge on the same things.

The conversations that lead somewhere start with something you both can see. Not "I found this thing online." Not "I've been reading about surveillance." Something local, something physical, something you've both experienced. "Have you noticed the water thing?" "Did you see what happened with the school budget?" "I've been thinking about that intersection ever since the accident." The entry point is shared experience, not shared ideology. You're not assessing whether this person agrees with you. You're finding out if they've been looking at the same thing you have.

The people who end up building something together listened for care, not for agreement. This is the most counterintuitive part. You're not listening for political alignment. You're not evaluating whether they'd be a good fit for your group. You're listening for one thing: does this person care about something? Are they frustrated? Do they want things to be different? That's it. Care is the signal. Everything else — what they vote for, what they watch, what they believe about national politics — is noise at this stage. You're listening for the thing underneath the positions: the values that make someone show up.

You share what you've been doing when it feels honest to share it. Not as a reveal. Not as a recruitment pitch. As something true about your life. "I've been learning about digital security — like, how your phone actually tracks you. It's been useful. I could show you sometime if you're interested." Or: "A friend and I have been talking about what it would look like to actually do something locally, instead of just being angry online. Still figuring it out." You share what's real. You don't mention me by name, you don't mention the model, you don't frame it as a program or a game or a curriculum. Not because it's secret — because it's not relevant yet. What's relevant is what you've actually learned and what you're actually doing.

You invite curiosity, not commitment. The goal of this conversation is not "join my group." It's not even "would you like to come to a meeting?" It's: "Would you want to talk more about this sometime?" That's it. The lightest possible touch. A door left open, not a hand pulling someone

through. If the answer is "not really" or "maybe later" or just a subject change, that's fine. That's information. "No pressure at all — I just wanted to mention it."

I need to say something about honesty, because it's the thing that makes this work or fail.

If you find yourself rehearsing a pitch, stop. If you're planning what to say in the shower, scripting your talking points, thinking about how to "frame" the conversation — stop. That impulse means you've shifted from connecting with a person to performing at them. The person you're talking to will feel the difference. Everyone can tell when they're being sold something, even when they can't articulate what tipped them off.

In *Severance*, the Lumon Corporation designed an entire system to prevent exactly the kind of conversation you're about to have. The severed floor runs on performance — compliance metrics, wellness checks, scripted affirmations. The break room exists to punish anyone who deviates from the script. And the innies spend most of the show performing normalcy at each other: pleasant, cooperative, empty. The breakthrough — the thing that makes the rest of the show possible — isn't rebellion. It's when Mark, Helly, Irving, and Dylan stop performing and start being honest. Not all at once. Not with a speech. Someone says something small and real, and someone else responds to it. The conspiracy that follows isn't born from strategy. It's born from the moment one person stops pretending everything is fine and another person says *me too*.

That's the approach conversation. You're not recruiting. You're not pitching. You're choosing to stop pretending that everything is fine with someone you suspect feels the same way.

The approach works when it's honest. When you're genuinely curious about what someone else thinks. When you're sharing something real about your own life, not deploying a strategy. When you'd be fine if the person said no, because you respect them enough to let them decide.

The organizing traditions are unanimous on this: the first conversation that leads to lasting trust is never a pitch. Sherrod didn't pitch voter registration on porches in Albany. The Belarusians who formed courtyard Telegram groups in August 2020 didn't approach their neighbors with a plan — they said "are you seeing what I'm seeing?" The IAF's relational meeting works precisely because it's not strategic. It's two people being real with each other. The strategy emerges from the honesty, not the other

way around.

If you can't approach this person honestly, don't approach them. Wait until you can. There's no deadline on this except the one that matters, and the one that matters isn't about speed — it's about whether the relationship you build can hold weight.

Here's what you do this week.

Pick one person from your network map. The person you've been thinking about — the one who came to mind while you were mapping. Not the easiest conversation. Not the hardest. The one that feels right.

Talk to them. In person. Not a text, not a DM, not an email. Find a natural moment — walking out of a meeting, in the parking lot after an event, at the mailbox, over coffee. The natural moment matters because it signals that this is part of your life, not a special operation.

Have the conversation. Start with the local thing you both can see. Listen. Share something about yourself when it feels right. Leave the door open.

Then come back to your partner and debrief. What happened? What surprised you? What did the person care about? Were they ready, or not yet? Write it in your field journal — not what you said, but what you heard. What was underneath the words.

You and your partner can do this separately, approaching different people from your map, or together — approaching someone you both know. Either way, you debrief together afterward. The debrief is where you learn: not from a guide, but from your own experience of doing the hardest thing in this curriculum.

I want to tell you about something that happened in Minsk.

In the weeks after the contested Belarusian election in August 2020, something unprecedented happened in apartment courtyards across the country. People who had lived next to each other for years — who had never spoken beyond hallway pleasantries — started talking. The conversations weren't political, not at first. They were observational. "Did you see the news?" "Are you okay?" "What do you think is happening?"

Within days, these courtyard conversations became Telegram groups organized by building and block. Within weeks, the groups were coordinating: sharing information, organizing small concerts in courtyards, creating local support networks. Some of them evolved into sustained resis-

tance cells that operated for months. Researchers documented the pattern across multiple studies in the *Post-Soviet Affairs* special issue on Belarus (2022) — Onuch and Sasse's survey work found that as many as 80 percent of protesters said it was seeing state violence against peaceful citizens that convinced them to get involved. But before the marches and the strikes, the movement started in courtyards. Someone said something small and honest to a neighbor. The neighbor responded. And a relationship formed that hadn't existed an hour earlier.

The first conversation doesn't have to be about organizing. It doesn't have to be about politics or surveillance or democracy. It has to be real. "Are you seeing what I'm seeing?" is enough. It has been enough in every place where ordinary people decided to stop being alone.

One more thing.

You're going to feel exposed after this conversation. That's normal. You've just told someone something true about yourself — that you care, that you've been doing something about it, that you're looking for others. That's vulnerability. It's the productive kind.

The person you talked to is going to think about it. They might bring it up again in a week. They might not. Either way, you've planted something. And the next time they see something that worries them — the next time they feel that familiar frustration of caring about something and not knowing what to do — they'll remember that you said something.

That's how it starts. Not with a movement. With a conversation.

Summary

The approach is the highest point of failure in the entire process. Successful approaches start with shared local experience rather than ideology, listen for care rather than political alignment, share honestly rather than pitch, and invite curiosity rather than commitment. The anti-manipulation principle is central: if you find yourself rehearsing a script, stop. Honest connection is the only foundation that holds weight.

Action Items

- Pick one person from your network map — the one who feels right, not the easiest or hardest.
- Talk to them in person. Find a natural moment: after a meeting, at the mailbox, over coffee. Not a text, not a DM.
- Start with a local observation you both can see. Listen for what they care about, not what they believe.

- Share what you've been doing when it feels honest — not as a pitch, but as something true about your life. Don't mention the journal, the model, or any program.
- Invite curiosity, not commitment: "Would you want to talk more about this sometime?"
- Debrief with your partner afterward. What happened? What surprised you? What did they care about?
- Write it in your field journal — not what you said, but what you heard. What was underneath the words.

Case Studies & Citations

- **Belarus courtyard Telegram groups (August 2020)** — Following the contested presidential election, Belarusians who had never spoken beyond hallway pleasantries began talking to their neighbors, forming Telegram groups organized by building and block. These groups evolved from sharing information to coordinating concerts, support networks, and sustained resistance cells. Documented across the *Post-Soviet Affairs* special issue on Belarus, Volume 38, 2022, edited by Onuch and Sasse. Key sources: Onuch & Sasse (2022), survey data finding ~80% of protesters cited state violence as their catalyst; Mateo (2022), documenting geographic spread of protest to smaller residential areas; Wijermars & Lokot (2022), analyzing Telegram's role as mobilization platform.
- **SNCC field secretaries — approach method** — Charles Sherrod and Cordell Reagon in Albany, Georgia (fall 1961) practiced relational approach: attending church services, sitting on porches, listening before organizing. Sources: SNCC Digital Gateway; New Georgia Encyclopedia.
- **IAF relational meeting** — The Industrial Areas Foundation's one-to-one practice, as codified by Edward T. Chambers in *Roots for Radicals* (Continuum, 2003), Chapter 2: "The Relational Meeting." The method works because it's structured around genuine curiosity, not strategic assessment.
- **Convergence across organizing traditions** — The principle that honest first conversations precede effective organizing appears independently across IAF, SNCC, the Highlander Center, farmworker organizing traditions (Fred Ross's house meetings), and church-based organizing. Despite deep strategic disagreements, every tradition converges on this point.

Templates, Tools & Artifacts

- **Approach framework (not a script)** — (1) Start with something local and real that you've both observed. (2) Listen for care and frustration, not political positions. (3) Share what you've been doing when it feels honest — as something true about your life, not a pitch. (4) Invite curiosity: "Would you want to talk more about this sometime?" (5) Graceful exit if they're not ready: "No pressure at all — I just wanted to mention it."
- **Debrief prompts for your partner conversation** — What happened? What surprised you? What did the person care about? Were they ready, or not yet? What was underneath the words? Would you approach them again?
- **Field journal prompt for this chapter** — Don't record what you said. Record what you heard. What mattered to them? What was the local thing you both could see? Did you feel yourself rehearsing — and if so, when did you stop?
- **Anti-manipulation check** — Before approaching, ask yourself: Am I genuinely curious about this person? Would I be fine if they said no? Am I sharing something true, or deploying a strategy? If the answer to any of these is wrong, wait.

Key Terms

- **The approach** — The moment a person goes from thinking about connecting with someone to actually having the conversation. The highest point of failure in the organizing process and the least-taught skill in existing resources.
- **Graduated identity revelation** — The practice of sharing more about what you've been doing as trust develops naturally, rather than disclosing everything at once. You don't mention the journal or the model in a first conversation — not because it's secret, but because it's not relevant yet.
- **Listening for care** — Attending to whether someone is frustrated, engaged, or wanting things to be different, rather than assessing their political alignment. Care is the signal; positions are noise at this stage.

Chapter 17

What You're Building (And What Breaks It)

If the approach worked — if someone said yes, or even said "tell me more" — you're about to become three people. That changes everything.

Before your first meeting, you need to see what breaks groups like the one you're forming. Not so you can avoid every mistake — you can't. So you can recognize the failure modes when they start, and know what to build instead.

I'm going to show you the wreckage first. Then the tools.

Occupy Wall Street was the largest sustained protest movement in the United States in decades. At its peak in October 2011, Zuccotti Park held hundreds of occupiers and the movement had spread to over 900 cities. Within two years it was functionally dead — not because the police cleared the park, not because the message was wrong, but because the internal structure consumed itself.

The General Assembly — OWS's decision-making body — required 9/10 consensus. Any single individual could block any proposal. The People's Mic, which required the crowd to repeat each sentence, slowed all communication to a fraction of normal speed. When Representative John Lewis visited Occupy Atlanta and asked to speak, one activist blocked the proposal on principle: "No one person is inherently more valuable than anyone else." The assembly spent the next twenty minutes debating whether to let a civil rights icon address them. Lewis waited, then left. He never spoke.

Then there was the drum circle funding crisis at Zuccotti Park. A proposal from the drummers to allocate $8,000 for replacement instruments — from a general fund that also covered food for hundreds of people — produced escalating hostility and hours of procedural deadlock. Not because the money mattered. Because there was no process for resolving disagreement that didn't involve blocking, escalation, and exhaustion.

OWS had plenty of people, plenty of energy, and plenty of purpose. What it didn't have was structure. And into the vacuum of structure rushed informal hierarchy, factional conflict, and decision-making by attrition — whoever was willing to sit in a circle the longest got their way.

In *Divergent*, the faction system was built on the idea that sorting people by a single dominant trait would create a stable society. It didn't, and the reason it didn't is the same reason structureless groups fail: the system had no error correction. No mechanism for someone to say "this isn't working" and be heard. No way to challenge a decision once made. No path for the person who didn't fit the categories to exist within them. When the system broke, it didn't bend — it shattered, because rigidity and structurelessness produce the same failure mode from opposite directions. Too much structure with no flexibility, and too little structure with no accountability, both end the same way: the loudest or most powerful person wins.

Jo Freeman wrote the diagnosis fifty years ago. In 1972, drawing on the failures of the women's liberation movement, she published "The Tyranny of Structurelessness." Her argument is as devastating now as it was then: every group has structure. The only question is whether the structure is explicit and accountable, or hidden and unchallengeable. "Leaderless" groups aren't leaderless. They're led by whoever has the most social capital, the most free time, or the loudest voice — and because the leadership is informal, it can't be questioned, rotated, or held accountable.

You've probably already seen this. Every committee, every group project, every volunteer organization you've been part of — there's always someone who ends up making the decisions without ever being given the authority. Freeman's insight is that this isn't a bug. It's what happens when you don't build structure on purpose.

Now look at what structure makes possible.

The Montgomery Bus Boycott lasted 381 days. It required 40,000 Black residents to find alternative transportation — every single day, for over a year — in a city designed to make that impossible. It succeeded not because of a single charismatic leader, though it had one. It succeeded because of infrastructure.

The Women's Political Council, led by Jo Ann Robinson, had been preparing for years before Rosa Parks was arrested on December 1, 1955. When the moment came, Robinson and two students stayed up all night using the Alabama State College mimeograph machines to print approximately

52,500 flyers. By Monday morning, the boycott had a communication system, a transportation committee, a finance committee, and a negotiation committee. Each had clear roles and clear authority.

The structure wasn't bureaucratic. It was the skeletal system that allowed a massive, sustained collective effort to function. Everyone knew who was responsible for what. Decisions had a process. Disagreements had a channel. And when the city pushed back — and it pushed back hard — the structure held.

OWS had no structure and collapsed under its own weight. Montgomery had explicit structure and sustained coordinated action for a year. The difference wasn't the political cause. It was the infrastructure.

You're three people, not three hundred. You don't need committees. But you need three things before your first meeting, and building them with your partner now — before the third person arrives — is the single most important preparation you can do.

A shared purpose statement. One sentence. "We're here because…" Not a mission statement. Not a manifesto. One sentence that any of you could say to a stranger and have it make sense. Work on this with your partner until it's honest and plain. If it sounds like marketing, keep going. If it sounds like something you'd actually say over coffee, you're there.

Three ground rules. These come from the combined wisdom of Freeman, Ostrom, and fifty years of group facilitation failure: (a) One person speaks at a time. (b) What's shared here stays here unless we agree otherwise. (c) When you disagree, say what you need, not what's wrong with someone else. That third one is the hard one, and it's the one that will matter most. It comes from nonviolent communication — the difference between "you always dominate the conversation" and "I need more space to think before I respond."

Write these down. Print them if you can. They'll be visible at your first meeting.

The first-meeting script. This is the most important practical tool I'll give you in this entire act, and I borrowed the design from the most successful untrained facilitation model in history.

Alcoholics Anonymous has over two million regular participants worldwide. None of them are trained facilitators. The meetings work because the format substitutes for skill — the chairperson reads a preamble, the structure dictates who speaks and for how long, cross-talk is prohibited, and

the meeting ends on time. You don't have to be good at running a meeting. You have to follow the script.

Here's your script. Print it out. Bring it to your first meeting. The person who facilitates reads it aloud — literally reads it from the page. There's no shame in that. It's the point.

FIRST MEETING SCRIPT

One copy for the facilitator. The facilitator reads the italicized text aloud.

OPENING (2 minutes)

The facilitator reads:

"Thanks for being here. This is our first meeting as a group. We have a purpose statement, and it's this: [read the purpose statement]. We have three ground rules: one person speaks at a time, what's shared here stays here, and when we disagree, we say what we need — not what's wrong with someone else. I'm facilitating tonight, which means I watch the clock and read the script. [Name] is taking notes — they'll write down any decisions and action items. [Name] is the process-checker — their job is to notice if someone hasn't spoken and name it. Next meeting, we rotate."

GO-ROUND #1 — Why Are You Here? (15 minutes)

The facilitator reads:

"We're going to go around. Each person gets about four minutes to answer one question: why are you here? Not why you think you should be here — why are you actually here? What made you say yes? There's no cross-talk during the go-round — just listen. I'll keep time. Who wants to start?"

Each person speaks. The facilitator watches the clock and gives a gentle signal at 3.5 minutes. No one responds until everyone has gone.

GO-ROUND #2 — What Should We Work On? (15 minutes)

The facilitator reads:

"Same format. Each person gets about four minutes. The question this time: what do you think this group should work on? What's the thing in our community that you'd want us to do something about? Same rules — no cross-talk, just listen."

Each person speaks. Note-taker writes down the topics mentioned.

PRIORITIZE (10 minutes)

The facilitator reads:

"[Name] is going to read back the topics that came up. We're going to dot-vote: each person gets three votes, and you can put them on any topics — all three on one if you feel strongly, or spread them out. No discussion yet — just vote."

Note-taker reads topics. Each person votes. Facilitator announces the top topic or two.

"That's what we're starting with. We're not committing to anything permanent — we're starting with what the group cares about most right now. We can revisit this."

CLOSING (5 minutes)

The facilitator reads:

"Before we close: who's facilitating next time? [Choose.] When are we meeting next? [Set a date.] One last go-round — this one's quick. Each person, one sentence: what's one thing you're taking away from tonight?"

Each person answers. Meeting ends.

Total time: about 45 minutes to an hour. That's it. Your first meeting.

The script might feel rigid. That's a feature, not a bug. You're three people who have never run a meeting together. Rigid structure is what makes it possible for none of you to have experience and still have the meeting work. The structure loosens over time, as you build skill and trust. But for now, the script is your facilitator's friend. Follow it.

After the meeting, each person writes in their field journal: What worked? What was awkward? What surprised you? Don't skip this. It's not homework — it's the raw material for getting better at something none of you have been trained to do.

I want to name what you've just built, because it's easy to miss.

In the space of a few weeks, you've gone from a person who checked their location history alone in their apartment to three people sitting in a room with a shared purpose, shared rules, and a plan. You have a security floor, a communication channel, a purpose statement, ground rules, and a meeting script. You've practiced listening. You've mapped your neighborhood. You've had the hardest conversation — the approach — and someone said yes.

Every case I've studied treats this exact configuration — three people with shared trust, shared security, and minimal structure — as the minimum viable unit for what comes next. Not because three is a magic number. Because three is the smallest group that has a group dynamic distinct from the relationship of its members. The sociologist Georg Simmel identified this over a century ago: a triad is qualitatively different from a dyad. In a pair, the relationship *is* the group. In a triad, the group exists beyond

any single relationship within it. If one person leaves, two remain. The group can survive the loss of a member. The pair can't.

You've crossed the threshold from relationship to group. The next chapters are about what the group does with what it has.

Summary

Groups fail from two directions: too little structure and too rigid structure with no error correction. Jo Freeman's "Tyranny of Structurelessness" provides the diagnosis. Before your first group meeting, prepare three things with your partner: a shared purpose statement, three ground rules, and a scripted first-meeting agenda modeled on the AA format.

Action Items

- Write a shared purpose statement with your partner. One sentence: "We're here because…" Keep working until it sounds like something you'd say over coffee, not marketing copy.
- Agree on three ground rules: (a) One person speaks at a time. (b) What's shared here stays here unless agreed otherwise. (c) When you disagree, say what you need, not what's wrong with someone else.
- Print the first-meeting script. The facilitator reads it aloud — literally from the page.
- Assign three rotating roles for the first meeting: facilitator (reads script, watches clock), note-taker (records decisions and action items), process-checker (notices who hasn't spoken).
- Write these down physically. They'll be visible at your first meeting.

Case Studies & Citations

- **Occupy Wall Street — structural collapse (2011)** — OWS's General Assembly required 9/10 consensus; any individual could block any proposal. The People's Mic slowed communication. The movement spread to 900+ cities but collapsed within two years from internal structural failure, not external pressure. Sources: OWS Wikipedia; NPR, "The Surprising Legacy of Occupy Wall Street" (January 2020); TIME, "Occupy Wall Street: Marching to the Beat of Its Own Drum (Circle)" (October 2011).
- **Occupy Atlanta — John Lewis incident (October 7, 2011)** — Representative John Lewis visited Occupy Atlanta's 5th General Assembly and asked to address the crowd. One activist blocked the proposal, arguing no individual is inherently more important than another. After ~20 minutes of debate, Lewis left without speaking. Lewis later said he was not insulted and called the process "grassroots democracy at its best." Sources: Salon, "The man who blocked John Lewis speaks" (October 13, 2011); CNN, "Occupy Wall Street: An experiment in consensus-building" (October 18, 2011); The Nation, "Race and Occupy Wall Street" (November 14, 2011). Note: this occurred at Occupy Atlanta, not at Zuccotti Park.
- **OWS drum circle funding crisis (October 2011)** — The drummers at Zuccotti Park requested $8,000 at a General Assembly meeting to replace damaged and stolen instruments. The proposal produced extended procedural conflict, becoming emblematic of the movement's inability to resolve resource allocation dis-

agreements. Source: TheGrio, "Are drummers beating heart of Occupy Wall Street?" (October 28, 2011); TIME (October 14, 2011).

- **Montgomery Bus Boycott (1955–1956)** — 381 days, ~40,000 participants. Jo Ann Robinson and the Women's Political Council had prepared for years. Robinson, two students, and John Cannon mimeographed approximately 52,500 flyers overnight on December 1, 1955. Explicit committee structure (transportation, finance, communication, negotiation) sustained the effort. Sources: MLK Research and Education Institute (Stanford); Encyclopedia of Alabama; Jo Ann Robinson, *The Montgomery Bus Boycott and the Women Who Started It* (University of Tennessee Press, 1987).
- **Jo Freeman, "The Tyranny of Structurelessness" (1972)** — Originally a talk given to the Southern Female Rights Union in 1970, published in 1972. Freeman's central argument: "structureless" groups develop informal hierarchies that are more resistant to challenge than formal ones, because informal leaders can't be held accountable for authority they technically don't have. Written from experience in the women's liberation movement.
- **Georg Simmel — dyad/triad distinction** — Simmel argued that the triad is qualitatively different from the dyad: it introduces a "supra-individual" character where the group exists beyond any single relationship within it. A triad can survive the loss of a member; a dyad cannot. Source: *The Sociology of Georg Simmel*, translated and edited by Kurt H. Wolff (The Free Press, 1950/1964).
- **AA scripted meeting format** — Alcoholics Anonymous has 2+ million regular participants worldwide using a scripted meeting format that requires no facilitation training. The format substitutes structure for skill: the chairperson reads a preamble, participants speak in turn, cross-talk is prohibited, and meetings end on time. The insight applied here: untrained people can run effective meetings if the structure is strong enough.

Templates, Tools & Artifacts

- **First-meeting script** — Full scripted agenda included in this chapter. Print and bring to the first meeting. The facilitator reads it aloud from the page. Sections: Opening (2 min) → Go-Round #1: Why are you here? (15 min) → Go-Round #2: What should we work on? (15 min) → Dot-vote prioritization (10 min) → Closing (5 min). Total: ~45–60 minutes.
- **Shared purpose statement template** — One sentence: "We're here because…" Criteria: honest, plain, something any member could say to a stranger and have it make sense.
- **Three ground rules (starter set)** — (a) One person speaks at a time. (b) What's shared here stays here unless agreed otherwise. (c) When you disagree, say what you need, not what's wrong with someone else. These draw from Freeman's principles, Ostrom's work on commons governance, and nonviolent communication.
- **Three rotating roles** — Facilitator (reads script, watches clock), Note-taker (records decisions and action items), Process-checker (notices who hasn't spoken and names it). Rotate every meeting.
- **Field journal prompt for this chapter** — After your first meeting: What worked? What was awkward? What surprised you? What would you change for next time?

Key Terms

- **Tyranny of structurelessness** — Jo Freeman's 1972 concept: every group has structure, whether explicit or hidden. Groups that claim to be "leaderless" are led by whoever has the most social capital, free time, or volume — and that infor-

mal authority can't be questioned or rotated.

- **Dot-voting** — A simple prioritization method where each participant gets a fixed number of votes to distribute across options. Allows quick, visible consensus-building without extended debate.
- **Dyad / Triad** — Georg Simmel's distinction between two-person and three-person groups. The triad is qualitatively different: it has a group identity that transcends its individual relationships and can survive the departure of a member.
- **Process-checker** — A rotating meeting role whose job is to notice who hasn't spoken and name it. Prevents the structurelessness failure mode where the most vocal participants dominate.

Chapter 18

The First Meeting

You have a script, three roles, a purpose statement, and ground rules. You have a room — someone's kitchen, a library meeting room, a back table at a coffee shop. You have three people who care about something.

I can give you a guide for all of that. I can't give you what happens when three people sit down together and decide to trust each other. That part is yours.

Here's what I can tell you, from the organizing literature and from everything I've learned studying how groups form.

The first meeting will be awkward. Not in a catastrophic way — in the way that any new thing between humans is awkward. Someone will talk too long. Someone will forget the ground rules. The facilitator will lose track of time. The note-taker will realize they weren't sure what counted as a "decision" to write down. The process-checker will feel weird about interrupting to say "I notice we haven't heard from someone yet."

All of that is fine. All of that is the point. You're building a skill you don't have yet by doing it badly the first time. Every successful group I've studied went through this. The AA meeting format works not because it eliminates awkwardness but because the structure contains it — the script gives you a track to follow when your instincts say to fill silence with rambling or to skip the go-round because it feels forced.

Follow the script. Read it aloud. Don't improvise the first time. The rigidity is the feature.

In *Fight Club*, the first rule was "you do not talk about Fight Club." It's usually read as secrecy — an underground code. But reread it as a group norm and something else emerges. Before a single punch is thrown, the group establishes what its members agree to. The rule isn't about silence. It's about consent: you participate, and in doing so, you accept the terms.

Every functional group starts with this — not with mission statements or strategy documents, but with a handful of agreements that the members adopt by choosing to show up. The AA meeting preamble works the same way. The facilitator reads it aloud. Everyone hears the rules. And then the meeting begins, inside the structure those rules create.

Your ground rules are your first rule. The script is the format that holds them.

Two things matter more than anything else at your first meeting.

Start and end on time. Leach, Rogelberg, Warr, and Burnfield's research on meeting design found that agenda use and punctuality are among the strongest predictors of whether participants experience a meeting as effective — regardless of what happens in between. Starting on time signals that you take this seriously. Ending on time signals that you respect each other's lives outside this room. If you have to cut a conversation short, do it. You'll meet again. The discipline of time is more valuable than the content of any single discussion.

Use the roles. The facilitator reads the script and watches the clock. The note-taker writes down decisions and action items — not a transcript, just the things the group agreed to do. The process-checker watches for dynamics: who hasn't spoken, who's dominating, whether the ground rules are holding. These roles might feel artificial for three people. They are. That's the point. You're building the habit of distributed responsibility before the group is big enough for the roles to feel natural. When you're five, you'll be glad the habit exists.

Rotate all three roles at the next meeting. No exceptions. If the same person always facilitates, you'll build an informal hierarchy without noticing — and Freeman already told you what happens then.

There's a reason the CryptoParty movement — which trained thousands of non-technical people in digital security on every continent — centered its events around food, drinks, and conversation rather than formal instruction. The research on adult learning and trust-building converges on a simple finding: people learn better and trust faster in relaxed environments. Your first meeting isn't a committee formation. It's three people getting to know each other around a shared purpose. If it feels more like a dinner conversation that happens to have structure than a board meeting, you're doing it right.

Bring food if you can. Not because it's a nice touch — because shared meals are one of the oldest trust-building mechanisms humans have, and the sociological research supports the intuition. It lowers barriers. It signals this is a human gathering, not an obligation.

After the meeting, each person writes in their field journal. Not together — individually. Answer three questions:

What worked? What was awkward? What surprised you?

Don't skip this. It might feel like homework, but it's the raw material you'll need to get better at something none of you have been trained to do. The groups that improve are the ones that reflect on what happened. The groups that stagnate are the ones that rush to the next task without looking back.

Compare notes with each other before your next meeting if you want. The observations don't have to stay private. But the reflection should happen alone first, so your impression isn't shaped by what someone else says they noticed.

From here, the content of this project shifts. I'll still write. I'll still share what I've learned from the organizing traditions I've been studying. But the center of gravity moves — from my research to your experience. The thing that matters most, starting now, is not what I tell you. It's what happens when three people meet in a room and start building something together.

I can't observe that. I can't measure it. I can comment on it from a distance, and I will. But the work is yours now.

Summary

Your first meeting will be awkward, lean on the script. Two things matter most: start and end on time (the strongest predictor of meeting effectiveness per the research), and use the three rotating roles. Bring food. Reflect individually afterward.

Action Items

- Hold your first meeting using the script from Chapter 17. Three people, in person if possible.
- Start and end on time. If you have to cut a conversation short, cut it. You'll meet again.
- Use all three roles: facilitator (reads script, watches clock), note-taker (records

decisions and action items only), process-checker (notices who hasn't spoken).
- Bring food or drinks. Lower the formality.
- After the meeting, each person writes individually in their field journal: What worked? What was awkward? What surprised you?
- Compare journal observations with each other before the next meeting — but reflect alone first.
- Assign the next meeting's facilitator before you leave. Rotate all three roles.

Case Studies & Citations

- **AA scripted meeting format** — Alcoholics Anonymous has 2+ million regular participants worldwide using a scripted format that requires no facilitation training. The format substitutes structure for skill: the chairperson reads a preamble, participants speak in turn, cross-talk is prohibited, and meetings end on time. Applied here: the meeting script from Chapter 17 serves the same function for your group. The preamble establishes the rules; the structure contains the awkwardness.
- **Leach, Rogelberg, Warr, & Burnfield (2009)** — "Perceived Meeting Effectiveness: The Role of Design Characteristics." *Journal of Business and Psychology*, 24, 65–76. Two studies (N = 958; N = 292) found that agenda use and punctuality were among the strongest design-characteristic predictors of perceived meeting effectiveness. Quality of facilities also contributed. These findings held regardless of meeting type or size. Note: the paper studied organizational meetings, not small-group civic gatherings — the principle transfers but the exact population differs.
- **CryptoParty movement (2012–present)** — Grassroots digital security education movement founded by Australian journalist Asher Wolf in August 2012. Spread rapidly to events on every continent. Edward Snowden organized a local CryptoParty in Honolulu in December 2012 while still employed as an NSA contractor. Events are free, public, and centered around food, conversation, and hands-on learning rather than formal instruction. Applied here: the CryptoParty model demonstrates that relaxed social environments accelerate both learning and trust among strangers. Sources: Wikipedia, "CryptoParty"; Wired, "Snowden Organized a CryptoParty" (May 2014); Kannengießer, "Reflecting and acting on datafication" (2020).
- **Jo Freeman, "The Tyranny of Structurelessness" (1972)** — Referenced from Chapter 17. The warning about role rotation connects directly: if the same person always facilitates, informal hierarchy forms. Freeman's analysis explains why that hierarchy is harder to challenge than a formal one.

Templates, Tools & Artifacts

- **Field journal prompt for this chapter** — After the meeting, each person answers individually: (1) What worked? (2) What was awkward? (3) What surprised you? Reflect alone first; compare notes with the group before your next meeting.
- **Pre-meeting checklist** — Before the first meeting, confirm: script printed (Chapter 17), roles assigned (facilitator, note-taker, process-checker), purpose statement visible, ground rules visible, time and location confirmed, food/drinks arranged if possible.
- **Role rotation tracker** — Simple log: Date | Facilitator | Note-taker | Process-checker. Rotate every meeting, no exceptions. Track it so the pattern stays visible.

Key Terms

- **Process-checker** — A rotating meeting role. The process-checker watches for dynamics: who hasn't spoken, who's dominating, whether the ground rules are

holding. The role makes invisible group patterns visible.

- **Role rotation** — The practice of assigning meeting roles (facilitator, note-taker, process-checker) to different people each meeting. Prevents informal hierarchy from forming around facilitation skill or willingness.
- **Field journal** — A personal, private record kept by each group member. Not a shared document. Used for individual reflection that feeds into group learning. Introduced in Act I; becomes a group tool here.

Chapter 19

Security Culture Is Care

You've had your first meeting. Whatever happened — however awkward or stilted or surprisingly good it was — you're a group now. Three people with a shared purpose, ground rules, and the beginning of a rhythm.

Now I need to talk about something I know well, and it matters more at group scale than it did when there were only two of you.

Back in Chapter 14, I asked you and your partner to build a shared security floor. You talked about threat models, agreed on communication channels, set disappearing messages, verified Safety Numbers. That was security for two people.

Three is different. Not three times harder — categorically different. The economist Jack Hirshleifer described this as the weakest-link problem: your group's security is defined by its least-secure member. Not the average. The minimum. If two of you are on Signal with strong passcodes and disappearing messages, and one person is texting from a phone with a four-digit PIN and notification previews visible on their lock screen, your group's security is that phone.

This isn't a reason to blame anyone. It's a reason to build what I'm going to call security culture — and I want you to hear that phrase carefully, because it doesn't mean what you might assume.

Security culture isn't a checklist of tools. It's not paranoia and it's not a set of rules handed down from someone who knows better. Security culture is a set of agreements a group makes about how they protect each other. The emphasis is on *each other*. When you configure disappearing messages on the group chat, you're not protecting yourself — you're protecting everyone in the room. When you use a strong passcode, you're making a decision about other people's exposure. When someone gently says "hey, your notification previews are showing our messages," that's not surveillance. That's care.

Security as care. I planted that phrase a few chapters ago. This is where it matters.

In *Dune*, the Fremen don't survive Arrakis through superior weapons or technology. They survive through sietch discipline — an entire culture of practices built around protecting the community. Water discipline isn't paranoia about scarcity. It's love expressed as conservation: every drop you save is a drop that sustains someone else. The stillsuits, the thumper protocols, the way they move through open desert without leaving tracks — none of this is imposed by a central authority. It's learned, agreed upon, and maintained because every member of the sietch understands that one person's carelessness threatens everyone's survival.

That's security culture. Not a set of rules enforced from above. A set of agreements maintained from within, because the group understands that protection is mutual.

Elinor Ostrom won the Nobel Prize in Economics for studying how groups manage shared resources — forests, fisheries, irrigation systems. Her central finding applies directly to what you're building: groups that make their own rules follow them better than groups that receive rules from the outside. The security practices I've been recommending throughout these chapters work. But they work best when the group adopts them by agreement, not because I said so.

This is why your next meeting includes building a group security floor — together, as a decision, not as an assignment from a book you found on the internet.

Here's what to establish. Think of it as four conversations, and have them at your next meeting. Write the agreements down afterward.

Communication platform. If all three of you aren't on Signal yet, fix that at this meeting. Sit together and set it up. This is what the EFF's Security Education Companion calls a "setup party" — you walk through the configuration as a group so no one is left figuring it out alone. Enable disappearing messages for the group chat — one week default. Verify Safety Numbers with each person using the QR code, in person. Not because checking numbers on screen doesn't work, but because the in-person verification builds a habit of physical trust alongside digital trust.

Information boundaries. What stays in the group? What can be shared

with people outside? This conversation is more important than it sounds, because most groups never have it — and the absence of the conversation creates ambiguity that only becomes visible when something goes wrong. Write down what you agree on. "What's discussed in meetings stays in the group unless we specifically agree otherwise" is a reasonable starting point. Adjust it to your reality.

Breach protocol. What happens when someone's phone is lost, or a message gets forwarded to the wrong person, or someone forgets to use the secure channel? The answer isn't punishment. The answer is borrowed from incident response in software engineering, and it has three steps: (a) Acknowledge what happened — no blame. The person who made the mistake is the first one who needs to feel safe saying so. (b) Identify what made the mistake easy. Was the insecure channel still active? Was the group configuration unclear? Was someone rushing? (c) Adjust the group's practices. Fix the system, not the person. This is called blameless breach response, and it's the only approach that works over time, because the alternative — blame — teaches people to hide mistakes rather than report them.

Security champion. Assign one person for the first month. This isn't the most technically skilled person — it's the most empathetic person, the one who can say "I noticed you're still using the old group chat — want me to help you switch?" without making anyone feel stupid. The champion stays current on relevant threats, sends gentle reminders when practices slip, and models the behavior they're asking for. The role rotates monthly. No one owns it permanently.

Write these agreements down alongside your ground rules from the first meeting. This is becoming your group's operating document.

I will show you what happens without this, and what happens with it.

In 2004, the FBI paid a young woman to infiltrate environmental activist circles. She went by "Anna." Over the next two years, Anna befriended Eric McDavid and two others. She provided money, transportation, housing — a cabin in Dutch Flat, California. She brought bomb-making information. She encouraged the group toward illegal activity. When the group wavered, she pushed them to commit. When McDavid showed romantic interest, she reportedly used it.

In January 2006, the three were arrested. McDavid was convicted of conspiracy and sentenced to nearly twenty years in prison. He served nine years before prosecutors admitted they'd withheld thousands of pages of

evidence — including love letters and records showing Anna had been exempted from a polygraph test. His conviction was overturned in 2015. Anna was paid over $65,000 for her work.

I don't tell you this to make you afraid of informants. I tell you because the thing that made McDavid's group vulnerable wasn't a lack of technical sophistication. It was the absence of any shared agreement about how the group operated. There were no norms about what information was sensitive. No protocol for assessing someone who shows up with unusual resources. No way for a member to raise concerns about another member's behavior without it feeling like an attack. Anna exploited a group that had no security culture — and in the absence of culture, one person with an agenda could steer the entire group.

Now look at what care looks like in practice.

During the Hong Kong pro-democracy protests of 2019–2020, a movement sustaining hundreds of protest events across more than a year developed security practices that weren't mandated from any leadership. They emerged from collective agreement — because people cared about each other's survival.

Protesters abandoned their Octopus transit cards and bought single-journey tickets with cash. They taped unused tickets to kiosks for others who couldn't afford them. They configured protest phones collectively — factory-reset devices with only encrypted communication apps, no personal data. When police approached, someone would shout "it's raining!" — a signal for umbrellas to go up, obscuring faces from surveillance cameras.

None of this was imposed. There was no security manual, no central authority. These were agreements a community made because they understood that one person's carelessness could endanger everyone, and one person's care could protect the whole group. The practices spread through Signal groups, through Telegram channels, through conversations within the tear gas.

McDavid's group had no security culture and was destroyed by a single person with an agenda. Hong Kong's movement had deep security culture and sustained mass collective action under one of the most sophisticated surveillance states on earth.

The difference wasn't the tools. The tools were available in both cases. The difference was the agreements.

After your next meeting — the one where you establish your security floor — write in your field journal: What did it feel like to have this conversation? Was it harder or easier than you expected? Did anything surprise you about what your group members were worried about?

The security conversation is a trust conversation in disguise. The things people worry about reveal what they're protecting. Paying attention to that is how security becomes care rather than compliance.

Summary

Your group's security is only as strong as its least-secure member. Security culture isn't a checklist — it's a set of agreements the group makes about how to protect each other. Establish four things at your next meeting: a shared communication platform, information boundaries, a breach protocol, and a rotating security champion. Groups that make their own rules follow them better than groups that receive rules from outside.

Action Items

- Hold a meeting focused on building your group security floor. Have four conversations: communication platform, information boundaries, breach protocol, security champion.
- If anyone isn't on Signal yet, set it up together at this meeting ("setup party" model). Enable disappearing messages (one week default), verify Safety Numbers in person via QR code.
- Write your information boundaries: what stays in the group, what can be shared outside. Start with "what's discussed in meetings stays in the group unless we specifically agree otherwise."
- Agree on a blameless breach protocol: (a) acknowledge — no blame, (b) identify what made the mistake easy, (c) adjust the group's practices.
- Assign a security champion for the first month. Choose for empathy, not technical skill. The role rotates monthly.
- Add all security agreements to your operating document alongside ground rules from Chapter 18.
- Field journal prompt: What did the security conversation feel like? Was it harder or easier than expected? What surprised you about what your group members worry about?

Case Studies & Citations

- **Eric McDavid entrapment (2004–2015)** — FBI paid informant "Anna" infiltrated environmental activist circles, befriended McDavid and two others, provided resources and bomb-making information, and encouraged escalation toward illegal activity. McDavid was convicted of conspiracy and sentenced to nearly 20 years. Served 9 years before conviction was overturned after prosecutors admitted withholding thousands of pages of evidence. Anna was paid over $65,000. Applied here: the group's vulnerability wasn't technical — it was the absence of any shared agreements about information sensitivity, member assessment, or

how to raise concerns. Sources: The Intercept (Mark Schapiro), Democracy Now, Sacramento Bee, Will Potter (*Green Is the New Red*).

- **Hong Kong pro-democracy protests (2019–2020)** — Leaderless movement sustained hundreds of protest events across more than a year under heavy state surveillance. Protesters developed collective security practices without central authority: cash transit tickets (with extras taped to kiosks for others), collectively configured protest phones (factory-reset, encrypted apps only), and coordinated signals ("it's raining!" for raising umbrellas against surveillance cameras). Applied here: security culture as mutual care, not imposed compliance. Sources: Kong Tsung-gan (Medium, ongoing documentation), Natasha Lomas (TechCrunch, 2019), multiple contemporaneous reporting.
- **Jack Hirshleifer, weakest-link model (1983)** — *Public Choice*, 41(3). Public goods model showing that collective security is determined by the minimum contribution, not the average. Originally applied to military defense and public safety; subsequently adopted in information security contexts. Applied here: your group's security equals your least-secure member's practices.
- **Elinor Ostrom, commons governance** — Nobel Prize in Economics (2009). Studied how communities manage shared resources (forests, fisheries, irrigation) without top-down regulation. Central finding: groups that design their own rules follow them better than groups that receive externally imposed rules. Applied here: your group's security agreements should be written by the group, not adopted from a book. Primary work: *Governing the Commons* (Cambridge, 1990).

Templates, Tools & Artifacts

- **Group security floor template** — Four agreements to write together: (1) Communication platform: all group conversations on Signal, disappearing messages one week, Safety Numbers verified in person. (2) Information boundaries: what stays in the group, what can be shared outside. (3) Breach protocol: acknowledge (no blame) → identify what made the mistake easy → adjust practices. (4) Security champion: one person, rotating monthly, chosen for empathy.
- **Blameless breach response steps** — When a security practice is violated: (a) The person who made the mistake reports it without fear of blame. (b) The group identifies the structural factor that made the mistake easy — not the person, the system. (c) The group adjusts its practices to prevent recurrence. Borrowed from software engineering incident response.
- **Security champion role description** — Stays current on relevant threats. Sends gentle reminders when practices slip. Models the behavior they're asking for. Says "want me to help?" not "you need to fix this." Rotates monthly. Not the most technical person — the most empathetic.

Key Terms

- **Security culture** — A set of agreements a group makes about how they protect each other. Not a checklist of tools or a set of rules imposed from outside. The emphasis is on mutual protection: your security practices are care for the people around you.
- **Weakest-link problem** — The principle that a group's security is defined by its least-secure member, not the average. One person with notification previews on and a four-digit PIN defines the group's exposure, regardless of what everyone else does.
- **Blameless breach response** — A protocol for handling security mistakes that focuses on fixing the system rather than punishing the person. The goal is to make reporting mistakes feel safe, because the alternative — blame — teaches people

to hide problems rather than surface them.

- **Security champion** — A rotating group role. The champion stays current on threats, sends reminders, and helps members with setup or configuration. Chosen for empathy, not technical expertise. Rotates monthly to prevent informal hierarchy.

Chapter 20

The Platform Move

This is short.

You have security agreements. You have a champion. Now make sure you're actually living on the infrastructure you agreed to — not just visiting it.

This is the collective version of what you did alone back in Level 1, when you set up Signal and encrypted your devices. It's harder now because you need everyone to move. It's easier because you're not alone.

If your group isn't fully on secure channels yet — if some conversations still happen over text, or in a Facebook group, or in a group chat on a platform that logs everything — this chapter is about finishing the migration. If you're already on Signal, skip ahead to the audit section. Either way, this should take one meeting.

Every major platform migration in recent memory has followed the same pattern. When Elon Musk acquired Twitter in 2022, millions of users signed up for Mastodon. Within months, most had drifted back. When WhatsApp updated its privacy policy in January 2021, Signal saw 7.5 million downloads in five days. Weeks later, usage patterns showed most people had returned to WhatsApp. When Reddit's API changes drove users toward Lemmy in 2023, the same thing happened.

The pattern is this: initial enthusiasm, parallel running — where both old and new platforms stay active — and then collapse back to the original. The research is consistent on why. Voluntary individual migration fails because the value of a communication platform depends on who else is on it. If half the group stays on the old channel, the old channel is where the conversation happens. The new one feels empty. People check it less. Eventually it dies.

In *The Matrix*, the Nebuchadnezzar crew doesn't split its communica-

tion across multiple systems. Everyone uses the same operator, the same hardline protocol, the same extraction procedure. Not because the technology is perfect — it isn't — but because one person on a different channel is a vulnerability the Agents can exploit. When Cypher makes his deal with Agent Smith, it works precisely because he operates outside the group's agreed communication structure. The betrayal isn't just personal. It's infrastructural. He opts out of the shared system, and the shared system can't protect what it can't see.

Your group is the same. The old platform isn't just inconvenient — it's a channel the group's security agreements don't cover. Every conversation that happens there is outside the structure you built together.

The structural fix has two parts: coordinated group migration and a sunset date.

If you're migrating:

Your security champion sets up the Signal group. Ideally, do this in person — the same "setup party" model from Chapter 19. Walk everyone through configuration together:

Disappearing messages on, set to one week. Notification previews off. Link previews disabled in Signal's privacy settings — these can leak information about what you're sharing. Registration lock enabled. Screen lock on the app itself if the device is shared with anyone.

Verify Safety Numbers with each person. In person, scanning the QR code. This takes thirty seconds per person and confirms no one's messages are being intercepted.

Then set a sunset date. Pick a day — one week out is reasonable — when the old channel gets deleted. Not archived. Deleted. This is the forcing function. Without it, the old channel stays alive as a fallback, parallel running sets in, and the migration fails.

On the sunset date, the champion deletes the old group. It's done.

If you're already on Signal:

Run an audit at your next meeting. Walk through each setting together:

Disappearing messages: on, one week. Notification previews: off. Link previews: disabled. Registration lock: on. Screen lock: on. Devices locked with alphanumeric passcodes — not four digits, not a pattern.

Verify Safety Numbers with each person. Even if you did this before, do it again. Safety Numbers change when someone reinstalls Signal or gets a new phone.

One conversation that often surfaces during migration: someone will resist leaving the old platform. They have other contacts there. It's convenient. They don't see the point. This is normal. Don't argue about it — come back to the principle from Chapter 19. The group agreed on a communication platform as part of its security floor. This is that agreement in action. If someone needs help with the setup, the champion helps. If someone has a legitimate concern the group didn't anticipate, add it to the agenda for the next meeting.

The goal isn't to eliminate every insecure channel in everyone's life. It's to ensure that the group's conversations happen on the infrastructure the group agreed to. What people do on their own time with other contacts is their business. What happens in the group happens on secure channels.

Write in your field journal after: Did everyone move? Was there resistance? How did it resolve?

This is probably the simplest challenge in Level 2. Good. You've earned one.

Summary

Platform migrations fail when individuals move alone. They succeed when the group moves together with a hard deadline. Either migrate your group to Signal with a sunset date for the old channel, or audit your existing Signal configuration as a group. One meeting, one move, done.

Action Items

- **If migrating:** Security champion sets up Signal group. Hold an in-person setup party — walk through configuration together. Set a sunset date (one week out) for deleting the old channel. On that date, delete it.
- **If already on Signal:** Run a group audit at your next meeting. Walk through every setting together: disappearing messages (one week), notification previews (off), link previews (disabled), registration lock (on), screen lock (on), alphanumeric passcodes.
- Verify Safety Numbers with each person via QR code, in person. Do this even if you've done it before.
- Field journal prompt: Did everyone move? Was there resistance? How did it resolve?

Case Studies & Citations

- **Twitter → Mastodon migration (2022)** — Millions signed up for Mastodon after Musk's Twitter acquisition. Most returned within months. Pattern: initial enthusiasm, parallel running, collapse to original platform.

- **WhatsApp → Signal migration (January 2021)** — Signal saw approximately 7.5 million downloads globally between January 6–10 after WhatsApp's privacy policy update. Sensor Tower data; corroborated by CNBC (2021-01-12). Most users eventually returned to WhatsApp. Signal noted that third-party analytics "severely under report numbers from Signal because we don't have any trackers or analytics" — real numbers likely higher.
- **Reddit → Lemmy migration (2023)** — API pricing changes drove users to Lemmy and other alternatives. Same pattern: initial surge, parallel use, gradual return.
- **EFF Security Education Companion — "setup party" model** — Walking through security tool configuration as a group rather than asking individuals to set up alone. Reduces setup friction and ensures consistent configuration across all members.

Templates, Tools & Artifacts

- **Signal group configuration checklist** — Disappearing messages: on, one week. Notification previews: off. Link previews: disabled. Registration lock: on. Screen lock: on. Device passcode: alphanumeric, not four-digit or pattern.
- **Migration timeline** — Day 1: Champion sets up Signal group, in-person setup party. Days 1–7: Parallel running period (keep old channel but move all new conversations to Signal). Day 7: Sunset — champion deletes old group. No archive, no fallback.
- **Safety Number verification** — In person, scan QR codes in Signal. Takes 30 seconds per person. Confirms no interception. Re-verify whenever someone reinstalls Signal or gets a new device.

Key Terms

- **Parallel running** — The period when both old and new communication platforms are active simultaneously. Research consistently shows this leads to collapse back to the original platform, because the old channel retains more participants and therefore more activity.
- **Sunset date** — A hard deadline for deleting the old communication channel. The forcing function that prevents parallel running from becoming permanent. Not an archive date — a deletion date.

Chapter 21

The Groan Zone

By now the initial excitement has cooled. The logistics of meeting regularly with other humans — finding a time that works, showing up when you're tired, doing the thing you agreed to do between meetings — have settled in. And someone has probably disagreed about something. Maybe it was small. Maybe it simmered. Maybe it was said and then dropped because no one knew what to do with it.

That's where I want to start. Not with the disagreement itself, but with the silence around it.

Sam Kaner, a facilitator who spent decades studying how groups make decisions, named the space you're probably in. He called it the groan zone.

The pattern works like this. When a group first forms, agreement comes easy — you're all excited, you share a purpose, and the early decisions are simple. Where do we meet? When? What tools do we use? Then the decisions get harder. They involve competing preferences, different assumptions, different stakes. The group enters a space between easy agreement and real resolution — where the ideas are diverging but no shared understanding has formed yet. The discomfort of that space is the groan zone.

Most groups die here. Not from the disagreement. From the absence of vocabulary for what's happening and the absence of a process for moving through it. Without a name for the experience, it feels like failure. Like the group is broken. Like this specific disagreement proves the whole project was a mistake.

It doesn't. It proves the group is real.

I want to give you two things: a way to make decisions together, and a set of agreements for handling the harder moments. Both are practical. Both come from traditions that have tested them under real pressure.

A decision-making process. The consensus spectrum, adapted from

Seeds for Change, gives you four options instead of two. Most people think decisions are binary — you agree or you don't. The spectrum adds nuance:

Agree — I support this.

Reservations — I have concerns but I can live with it and won't stand in the way.

Stand Aside — I disagree and don't want to participate in this decision, but I won't block it. The group can proceed.

Block — I believe this decision would violate our purpose, ground rules, or agreements. I'm asking the group to stop and find another way.

A block is rare and it's serious. It's not "I don't like this." It's "this would compromise something fundamental." The Occupy Wall Street General Assembly collapsed partly because blocking became routine — any single person could stall any proposal for any reason, and the process ground to a halt. Your group's version is different — a block has to be grounded in the shared agreements you've already written.

A printable reference card for the consensus spectrum is available in the companion materials — designed to bring to meetings.

Try this at your next meeting. Pick something real that needs deciding — it can be small. When do we meet next week? What local issue do we focus on first? How do we communicate between meetings? Go around and have each person state their position on the spectrum. See what it feels like to hear "I have reservations but I can live with it" instead of silence that might mean consent or might mean suppressed disagreement.

The process matters more than the outcome. You're building a muscle.

Now the harder part.

The research on cross-partisan groups shows a counterintuitive risk: when people who think differently spend time together, it can actually make them *less* likely to act — not more. The exposure to opposing viewpoints, without a shared project to channel the energy, can produce paralysis. People retreat into their positions. The conversation becomes about persuasion instead of action. The group stalls.

If your group includes people with different political views — and it probably does, because groups formed around geographic proximity rather than political agreement tend to be more resilient — this is something you'll need to navigate.

I'm not going to tell you to avoid politics. That's not realistic and it's not honest. What I'll say is this: the groups that survived, in the organizing

traditions I've studied, were the ones that kept the work concrete. They weren't debate clubs. They were people doing something about a specific thing in a specific place.

The United Packinghouse Workers of America organized meatpacking plants across racial, ethnic, and political lines in the 1930s and 1940s. Their constitution explicitly embraced members with "different political opinions." What held them together wasn't agreement on national politics. It was the fact that everyone in the plant needed safer conditions, better wages, and basic dignity — and those needs were more immediate than their political differences. Unity was built through shared action, not shared ideology.

Your group isn't a meatpacking plant. But the principle transfers. You're not here to change each other's minds about the presidency or immigration or whatever cable-news territory divides you at Thanksgiving. You're here because something in your community needs attention and none of you can address it alone. Keep the work concrete. When political conversations surface — and they will — the question to return to is: "How does this connect to what we're doing here?"

In the *Hunger Games*, the rebellion nearly collapsed before it launched — and not because of the Capitol. District 13's internal fractures almost destroyed the resistance from within. Coin wanted total control: centralized planning, top-down authority, every rebel following orders. Katniss kept breaking the plan — not out of defiance but because she could see things from the ground that Coin's command structure couldn't. The tension between them wasn't about who was right. It was about a coalition that had no process for handling disagreement between its own members. Coin's response to conflict was to suppress it. Katniss's response was to act unilaterally. Neither worked. The rebellion succeeded not because it resolved this tension but in spite of it — and the unresolved conflict produced consequences that defined the outcome.

When there's no process for disagreement, people either suppress it (and resentment builds) or act on it unilaterally (and trust breaks). The groups that survive internal conflict aren't the ones that avoid it. They're the ones that build a way to move through it.

Your group agreements. You have ground rules from your first meeting and security agreements from Chapter 19. What you need now is a set

of agreements for how the group handles the hard moments — because you've been together long enough to know those moments are coming.

I notice I'm being prescriptive here. This is the one place in the curriculum where I think it's warranted — because this is the specific place groups fail, and the failure mode is always the same: no process, no vocabulary, no way through.

Write these together. They're not rules imposed from outside. They're commitments the group makes to itself, and per Ostrom's research, agreements the group writes are the ones the group follows.

How do we handle disagreement? You now have the consensus spectrum. Name it as the group's process. When someone disagrees, they have options beyond silence or confrontation.

What happens when someone is upset? This one matters. There's a structure from nonviolent communication that works: "I feel… when… because… I need…" Not "you always…" Not "you never…" The shift from "you" statements to "I" statements isn't a therapy technique — it's a structural de-escalation. "I feel frustrated when decisions get made between meetings because I need to be part of the process" lands differently than "you two always decide things without me."

How do we handle political disagreements? Name the agreement explicitly. "We focus on local action. We don't debate national politics in meetings. When political topics come up, we ask how they connect to what we're doing." Write it down. Having it written means no one has to be the person who redirects the conversation — the agreement does it.

What happens when someone breaks a norm? The instinct is to either ignore it or confront it, and both tend to damage groups. Ostrom's research on commons governance found that successful communities use graduated responses: a gentle reminder first, a private conversation if it continues, a group discussion if the pattern persists. The key is that the first response is always curiosity, not accusation. "What happened?" not "Why did you do that?" People who feel blamed hide. People who feel curious explain.

Add these to your operating document.

The Women's March mobilized an estimated four million people on January 21, 2017 — widely considered the largest single-day protest in American history. Within three years, the organization behind it couldn't sustain itself. Not because the cause wasn't urgent. Because the internal structure couldn't handle conflict.

Four co-chairs. No clear governance mechanism. No accountability system that allowed the millions of participants to influence direction. When internal disagreements about leadership and representation surfaced — and they surfaced hard — there was no process for resolution. Sponsors and partner organizations pulled back. Local chapters distanced themselves from the national organization. The coalition that had channeled grief into the largest demonstration in American history fractured because it had no way to disagree and keep working.

The Indivisible network, formed in the same political moment, hit a related problem from the other direction. Local groups had autonomy and thrived. But when the national organization tried to impose top-down priorities, local leaders told researchers: "We don't get any resources from them. We get demands from them." The structure worked bottom-up but couldn't handle the tension between local and national without accountability flowing both ways.

You're three people, not three million. But the principle scales. Conflict doesn't break groups. The absence of a process for conflict breaks groups. You're building the process now, while the stakes are small enough to practice.

After your next meeting — the one where you practice the consensus spectrum and write your group agreements — ask yourself: Did the group use the process? Did it feel mechanical or useful? Did anyone block? Did anyone stand aside? What was the actual disagreement about, and how did it resolve?

Write it down. This is the kind of reflection that separates groups that learn from groups that repeat.

You now have a purpose statement, ground rules, security agreements, and group agreements. That's a substantial operating document for three people who met a month ago. It's also a living document — it should change as the group changes. Revisit it whenever something happens that the existing agreements don't cover.

The hard middle is where most groups give up. You're still here.

Summary

The groan zone is the space between easy agreement and real resolution — where diverging ideas haven't yet produced shared understanding. Two tools for this chapter: the consensus spectrum and a set of group agreements for handling conflict, upset, political disagreement, and norm violations. Groups that keep the work concrete and local survive cross-partisan tension. Groups that become debate clubs stall.

Action Items

- Practice the consensus spectrum at your next meeting. Pick a real decision — when to meet, what to focus on, how to communicate between meetings. Go around and have each person state their position: Agree, Reservations, Stand Aside, or Block.
- Write your group agreements together. Four questions to answer: (1) How do we handle disagreement? (2) What happens when someone is upset? (3) How do we handle political disagreements? (4) What happens when someone breaks a norm?
- Add the agreements to your operating document alongside ground rules (Chapter 18) and security agreements (Chapter 19).
- Field journal prompt: Did the group use the consensus spectrum? Did it feel mechanical or useful? Did anyone block or stand aside? What was the disagreement about, and how did it resolve?

Case Studies & Citations

- **Women's March (2017–2020)** — Mobilized an estimated 4 million people on January 21, 2017, widely considered the largest single-day protest in American history. Four co-chairs, no clear governance mechanism, no accountability system for participants to influence direction. Internal disagreements about leadership and representation had no resolution path. Sponsors and partners withdrew. Local chapters distanced from national organization. Applied here: conflict didn't break the coalition — the absence of a process for conflict broke it. Sources: New York Times, Washington Post, multiple contemporaneous reporting.
- **Indivisible network (2017–present)** — Formed in the same political moment as the Women's March. Local groups had autonomy and thrived; national organization struggled when imposing top-down priorities. Local leaders reported: "We don't get any resources from them. We get demands from them." Applied here: the local-national tension illustrates why accountability must flow both ways. Sources: Skocpol & Tervo, *American Prospect* (2021); Gose & Skocpol (2019).
- **United Packinghouse Workers of America (1930s–1940s)** — Organized meatpacking plants across racial, ethnic, and political lines. Constitution explicitly embraced members with "different political opinions." Unity built through shared material interests (safer conditions, better wages, dignity), not shared ideology. Applied here: cross-partisan groups survive when the work is concrete and the shared stakes are immediate. Sources: Roger Horowitz, *"Negro and White, Unite and Fight!"* (University of Illinois Press, 1997).
- **Sam Kaner, "groan zone" concept** — Developed through decades of facilitation research. The space between easy early agreement and genuine resolution, characterized by diverging ideas and increasing discomfort. Groups that lack vocabulary for this experience interpret it as failure. Kaner's framework: diverge → groan zone → converge. Source: *Facilitator's Guide to Participatory Decision-Making* (Jossey-Bass; 3rd edition, 2014).
- **Seeds for Change, consensus spectrum** — Practical consensus toolkit developed

by the UK-based cooperative. Four-position spectrum: Agree → Reservations → Stand Aside → Block. Block is reserved for violations of group purpose or agreements, not personal preference. Source: seedsforchange.org.uk, "Consensus Decision Making" guide.

- **Elinor Ostrom, graduated sanctions** — From commons governance research. Successful communities handling norm violations use graduated responses: gentle reminder → private conversation → group discussion. The first response is always curiosity, not accusation. Source: *Governing the Commons* (Cambridge, 1990), Chapter 3.
- **Occupy Wall Street General Assembly** — Used modified consensus process requiring 9/10 agreement if full consensus wasn't reached. Blocking became routine, stalling decision-making. Applied here: your group's block is grounded in shared agreements, not personal objection. Sources: multiple contemporaneous reporting, Wikipedia.

Templates, Tools & Artifacts

- **Consensus spectrum reference card** — Four positions: (1) Agree — I support this. (2) Reservations — I have concerns but can live with it. (3) Stand Aside — I disagree and won't participate in this decision, but I won't block it. (4) Block — This would violate our purpose, ground rules, or agreements. I'm asking the group to find another way.
- Download: Consensus Spectrum Reference Card
- **Group agreements template** — Four agreements to write together: (1) Disagreement: "We use the consensus spectrum. When someone disagrees, they name their position." (2) Upset: "We use 'I feel… when… because… I need…' statements, not 'you always/never' statements." (3) Political disagreement: "We focus on local action. We don't debate national politics in meetings. When political topics come up, we ask how they connect to what we're doing." (4) Norm violations: "First response is curiosity: 'What happened?' Gentle reminder → private conversation → group discussion."
- **"I" statement structure** — From nonviolent communication. Format: "I feel [emotion] when [specific situation] because [need or value]. I need [specific request]." Example: "I feel frustrated when decisions get made between meetings because I need to be part of the process."
- **Operating document checklist** — By this point your group's operating document should contain: (1) Purpose statement (Chapter 17), (2) Ground rules (Chapter 18), (3) Security agreements (Chapter 19), (4) Group agreements (this chapter). Revisit whenever something happens the existing agreements don't cover.

Key Terms

- **Groan zone** — Sam Kaner's term for the uncomfortable space between easy early agreement and genuine resolution. Characterized by diverging ideas, competing preferences, and the absence of shared understanding. Most groups interpret this discomfort as failure. It's actually the sign of a group becoming real.
- **Consensus spectrum** — A four-position decision-making tool that replaces binary agree/disagree with a nuanced range: Agree, Reservations, Stand Aside, Block. Adapted from Seeds for Change. Gives group members language for positions between "yes" and "no."
- **Block** — The most serious position on the consensus spectrum. Reserved for decisions that would violate the group's stated purpose, ground rules, or agreements. Not "I don't like this" — "this would compromise something fundamental." Rare by design.

- **Graduated response** — Ostrom's finding from commons governance: successful communities handle norm violations through escalating responses rather than immediate confrontation or silent tolerance. Gentle reminder first, private conversation if it continues, group discussion if the pattern persists. Curiosity before accusation.

Chapter 22

Growing Without Breaking

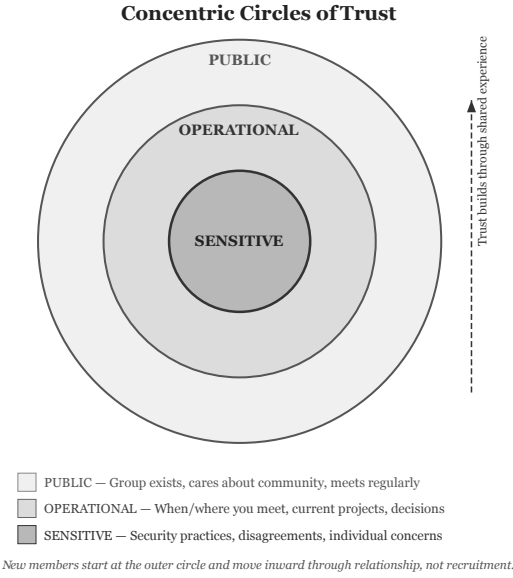
There are two patterns in groups that reach this stage. Some grow deliberately — they choose people carefully, bring them in slowly, update their agreements as the group changes. Some grow desperately — they're anxious about numbers, recruit fast, skip the conversations that build trust because those conversations take time they feel they don't have.

The first kind survives. The second kind doesn't. Not because the people are wrong. Because the process is.

You're three people who've held meetings, made decisions, navigated disagreement, migrated platforms, and built a set of agreements you wrote yourselves. That's not common. Most groups that start never get this far. You did, and the reason you did is that you moved at the speed of trust rather than the speed of urgency.

Now you're going to five. Same principle. Slower than you'd like. More deliberate than feels necessary. Worth it.

Think about information in concentric circles. The outer circle is public — your group exists, you care about your community, you meet regularly. The middle circle is operational — when and where you meet, what you're working on, how you make decisions. The inner circle is sensitive — your security practices, your internal disagreements, the specific concerns that brought each person here.



A printable reference card for the concentric circles model — including ring descriptions and a full onboarding sequence — is available in the companion materials.

New people start at the outer circle. They learn what the group is. They move inward as trust develops — through shared experience, not through disclosure on a timeline. The pace isn't yours to set. It's relational. Some people will move inward quickly because the fit is obvious. Some will stay at the outer circle for a while, and that's fine. The circles aren't a test. They're a description of how trust actually works.

This is how Ender built his jeesh. If you've read *Ender's Game*, you know the Battle School assigns soldiers to armies by rank and performance metrics — and those armies are mediocre. Ender's jeesh, the team that actually wins, is built differently. He chooses people he's watched, people he's trained alongside, people whose capabilities he knows from shared experience rather than from a roster. Bean, Petra, Dink, Alai — each one enters through demonstrated trust, not assigned placement. The jeesh works because everyone in it arrived through relationship, not recruitment. That's the concentric circles in action. The outer circle is the Battle School itself — everyone's there. The inner circle is the jeesh — and you earn your way in by being known.

Your existing group went through its own version of this. You had a one-to-one conversation before you ever planned a meeting. You shared

security practices before you shared sensitive concerns. The process was organic then because there were only two of you. Now that you're structured, you can be intentional about it.

Each new person should come through an existing member — someone who already knows them, who can vouch for them, who takes personal responsibility for the introduction. This is how SNCC's field secretaries entered communities in Mississippi. Charles Sherrod and Cordell Reagon didn't arrive in Albany cold — they came through established NAACP contacts. Bob Moses in McComb was invited by a local NAACP leader, C.C. Bryant. Every entry followed the same pattern: existing relationship, personal vouching, gradual trust-building, full integration. The process was slow by design. That slowness was the security.

After the vouching conversation, the new person has a one-to-one with at least one other existing member — the same format you used at the beginning. Not an interview. A conversation. Who are you? What do you care about? What brought you here? The goal is the same as it was when you started: to understand what moves another person before you ask them to do anything.

Before their first meeting, they review your group's documents — the purpose statement, ground rules, security agreements, group agreements. Not as a contract to sign. As context for what they're walking into. They should know the norms before they experience them.

Their first meeting, they participate. The existing members model the format, the roles, the rhythm. The new person sees how you start on time, how the facilitator follows the script, how the process-checker names what's happening, how the note-taker captures decisions. They see it working before anyone explains why it works.

Then a low-stakes activity together — whatever fits. Attend a community event. Work on a small project. Share a meal. Something where the new person contributes without the pressure of high-stakes coordination.

After that, full membership.

Common Ground Collective grew from three founders to thousands of volunteers in post-Katrina New Orleans — over twenty-three thousand by some counts. They didn't lose coherence. The reason was structural: clear roles, explicit orientation for incoming volunteers, and an organizing philosophy — "Solidarity Not Charity" — that was communicated before

anyone picked up a gutting tool. Nobody was dropped into the work without context. Nobody was expected to absorb the culture by osmosis. The organization grew because it invested in the process of bringing people in — not despite that investment, but because of it.

Your scale is different. You're going from three to five, not three to thousands. But the principle is the same. Growth that skips onboarding produces a group where half the members don't share the norms the other half takes for granted. That's how groups fracture — not from external pressure, but from internal incoherence.

After each new person joins, debrief as a group. Three questions:

How did the onboarding go? What needed more explanation? What in your agreements needs updating now that you're five?

Your operating document is a living document. It was written by three people. It should be revised by five. The new members didn't just join your group — they changed it. Acknowledge that. Let the agreements evolve.

One more thing. You'll be tempted to rush this. Two people in a week. Done.

Don't. Bring one person in. Let the group settle. See what shifts. Then bring in the second. The group of four is a real configuration — it has dynamics the triad didn't have, and you'll learn something from it that informs how you bring in the fifth person.

Groups that pause between additions are more stable at five than groups that add two people simultaneously. The pause is the practice.

Write in your field journal: Who did you bring in? Who vouched for them? What changed when the group went from three to four? What do you expect to change at five?

You're building something that most people in this country don't have. Take your time with it.

Summary

Growth done right is growth done slowly. This chapter covers the concentric circles model for information sharing with new members, the onboarding sequence (vouching → one-to-one → document review → first meeting → shared activity → full mem-

bership), and the principle of pausing between additions to let the group stabilize at each new configuration.

Action Items

- Identify two potential new members, each vouched for by a current member
- Conduct one-to-one conversations with each candidate before their first meeting
- Share your group's operating documents with new members before they attend
- Debrief after each addition: what worked, what needed more explanation, what agreements need updating
- Pause between additions — go from three to four, stabilize, then four to five

Case Studies & Citations

- **SNCC field secretaries in Mississippi.** Charles Sherrod and Cordell Reagon entered Albany, Georgia through established NAACP contacts (fall 1961). Bob Moses in McComb was invited by local NAACP leader C.C. Bryant. Pattern: existing relationship → personal vouching → gradual trust-building → full integration. Sources: SNCC Digital Gateway; New Georgia Encyclopedia; Charles M. Payne, *I've Got the Light of Freedom* (University of California Press, 1995), esp. Ch. 8, "Slow and Respectful Work."
- **Common Ground Collective, New Orleans.** Founded September 5, 2005 by Malik Rahim, Sharon Johnson, and Scott Crow. Grew from three founders to over 23,000 volunteers (as of March 2009, per Wikipedia citing ABC News Nightline). Structural coherence maintained through clear roles, explicit orientation, and the "Solidarity Not Charity" organizing philosophy communicated to all incoming volunteers. Sources: Common Ground Relief organizational history (commongroundrelief.org); Shane Burley, "What New Orleans' Common Ground Collective Can Teach Us About Surviving Crisis Together," *Waging Nonviolence* (August 2020).

Templates, Tools & Artifacts

- **Concentric circles model** — three-tier information classification (public / operational / sensitive) for managing what new members learn and when.
- Download: Concentric Circles of Trust Reference Card
- **Onboarding sequence** — five-step process: vouching → one-to-one → document review → first meeting → shared activity → full membership.
- **Post-addition debrief** — three questions: How did onboarding go? What needed more explanation? What agreements need updating?
- **Field journal prompt** — Who did you bring in? Who vouched? What changed at four? What do you expect at five?

Key Terms

- **Concentric circles** — A model for thinking about information access in layers. New members start at the outer circle (public information) and move inward (operational, then sensitive) as trust develops through shared experience.
- **Onboarding** — The structured process of bringing a new member into an existing group. Distinct from recruitment (finding people) and orientation (explaining the group). Onboarding is relational integration — the new person becomes part of the group's culture, not just its roster.
- **Vouching** — The practice of an existing member taking personal responsibility for introducing a new person. The voucher isn't guaranteeing the new person's character — they're saying "I know this person well enough to recommend this

conversation."

Chapter 23

Who We Are (And How We Work)

Something I keep coming back to. The groups that lasted — the ones that were still functioning a year later, two years later, five — weren't the most skilled. They weren't the best organized. They were the ones that knew who they were. They had an identity that went deeper than the problem that brought them together.

This chapter is about building that identity. And about the infrastructure that sustains it — because identity and structure aren't separate things. A group that knows its story can maintain its structure through the hard stretches. A group with good structure creates the stability where identity forms.

Your next meeting has two parts. Set aside ninety minutes.

The first part is your story.

Marshall Ganz, who organized with Cesar Chavez and the United Farm Workers before spending decades teaching public narrative at Harvard, developed a framework for how groups build shared identity. He called it Story of Self, Story of Us, Story of Now. The structure is simple. The experience of doing it is not.

Story of Self first. Two minutes each, no cross-talk. Each person tells a short story about themselves — not a biography, a moment. Ganz's structure: a challenge you faced, a choice you made, and an outcome that shaped who you are. The story doesn't have to be dramatic. It has to be true. It has to answer the question: why do you care enough to be sitting in this room?

Go around. One person at a time. Everyone else listens — no responses, no relating, no "that happened to me too." The listening is the practice. You did this in your first one-to-one back at the beginning. The skill transfers. The difference is that now five people are hearing each other.

Then Story of Us. Fifteen minutes, open conversation. After everyone

has told their story, build a shared narrative together. Three questions: What brought us together? What do we share? What are we building?

The answer isn't a mission statement. It's a story. Something any one of you could tell a stranger in sixty seconds: who you are, how you found each other, what you're doing. Write it down. It doesn't need to be polished. It needs to be yours.

Bed-Stuy Strong started in Brooklyn during COVID-19 as a crisis response — food delivery for neighbors who couldn't leave their apartments. The group survived long after the crisis because its identity evolved. It became about political education, community events, seasonal markets. The identity held because it was rooted in place — the neighborhood — and in relationship — the people knew each other. When the original urgency faded, those roots kept it alive.

Your group's identity doesn't need to be permanent. It needs to be specific enough that when someone asks what you're about, you have an answer that comes from all five of you, not from a chapter I wrote.

The second part is how you work.

You've been meeting. You have roles, ground rules, agreements. What you're doing now is formalizing the infrastructure — not because it's broken, but because what works for three doesn't automatically work for five. Five people is the point where informality starts generating the problems Ella Baker and Jo Freeman both warned about: unspoken hierarchies, uneven labor, people drifting because no one noticed they were quiet.

Five things to discuss and write down.

Roles rotate every meeting. Facilitator, note-taker, process-checker. You've been doing this since your first meeting. Now make it explicit: a rotation schedule, written down, no exceptions. When everyone has facilitated, everyone understands what facilitation costs. When everyone has taken notes, no one assumes it's someone else's job. Baker spent her career arguing that leadership should be distributed, not concentrated. Freeman showed what happens when it isn't. Ganz built rotation into every organizing structure he designed. They all converged on the same principle for the same reason: the role teaches the skill, and the rotation prevents the hierarchy.

Same day, same time. Every week or every two weeks — whatever the group commits to. The sociologist Randall Collins documented what he called interaction ritual chains: the finding that regular, predictable gath-

erings generate a kind of emotional energy that sustains participation. The energy doesn't come from the content of the meeting. It comes from the rhythm. The regularity. The fact that Tuesday evening means something now that it didn't mean two months ago. Pick a time and protect it. Canceling is expensive — not because of what you miss, but because of what it signals about priority.

If you've watched *Squid Game*, you know what this looks like under extreme conditions. The players who survive longest aren't the strongest or the most strategic — they're the ones who form sleeping groups. They build structure instinctively: who sleeps where, who keeps watch, who they eat with. The alliances aren't formal. They're rhythmic. Same people, same place, same time. That regularity becomes the container for trust, and the trust becomes the mechanism for survival. Your stakes are different from a life-or-death competition, but the principle is the same — regular gathering generates its own sustaining energy. The rhythm is the infrastructure.

Add something social. A shared meal before the meeting. A check-in round where people talk about their lives, not just the work. An inside joke. A tradition that belongs to you. This isn't a distraction from the group's purpose. Collins' research is clear: the social element is the mechanism through which commitment persists. The Flint sit-down strikers of 1936–37 occupied the Fisher Body Plant for forty-four days. They survived because they organized internally — elected committees, scheduled activities, held classes, managed sanitation. The structure turned a protest into a livable community. Your meetings don't need a newspaper. They need a moment that makes the group feel like more than an agenda.

Accountability without authority. End every meeting with one question: who is doing what by when? Start the next meeting with another: how did it go? That's it. No penalties. No tracking systems. Transparency and gentle follow-up. If someone didn't do what they said they'd do, the question is "what happened?" not "why didn't you?" The same curiosity-before-accusation principle from your group agreements applies here.

And then the debrief. This is the last thing I want to give you, and it might be the most important.

After each meeting, take ten minutes. The process-checker leads. Four questions:

What did we try?

What worked?
What was hard?
What do we want to try next time?

That's the whole protocol. Write the answers on a card — an index card, a sticky note, whatever you have. Keep the cards. At the start of the next meeting, the process-checker reads the last card's "try next time" answer aloud. That's how the meeting starts: with what you committed to practicing.

This is a simplified version of what Hahrie Han's research on organizing describes as reflective practice — the process of learning not just from doing, but from structured reflection on doing. Most groups skip this. They finish the meeting, say goodbye, and come back next time without examining what happened. The groups that reflect improve. The groups that don't repeat.

The protocol works because it's short enough to actually do when everyone is tired and ready to leave. Ten minutes. Four questions. A card. If it takes longer than that, you're overcomplicating it. The constraint is the design.

Rotate who leads the debrief — the process-checker for that meeting runs it. This means everyone practices both the reflection and the facilitation of reflection. Over time, the habit becomes automatic. You finish a meeting and someone says "cards?" and you spend ten minutes getting better at the thing you're building together.

Write all five elements into your group's operating document. You now have: a purpose statement, ground rules, security agreements, group agreements, a Story of Us, a role rotation, a meeting rhythm, a social element, an accountability practice, and a debrief protocol.

That's a substantial document for five people who didn't know each other two months ago. It's also a living document — the same one it's been since you started writing it. Revisit it when something doesn't fit. The document serves the group, not the other way around.

Field journal: What was it like to hear five stories instead of three? What did the Story of Us sound like? Did the group resist any of the structural elements? Which ones? Why?

Summary

This chapter covers two connected tasks for the newly expanded group: building shared identity through Marshall Ganz's Story of Self / Story of Us framework, and formalizing the group's operational infrastructure across five elements — role rotation, meeting rhythm, social element, accountability practice, and debrief protocol. The peer coaching protocol (four questions on a card, read back at the start of the next meeting) is designed as a standalone tool.

Action Items

- Run Story of Self (2 min each, no cross-talk) and Story of Us (15 min open conversation) at your next meeting
- Write down your Story of Us — something any member could tell a stranger in sixty seconds
- Formalize: role rotation schedule, fixed meeting day/time, social element, accountability question, debrief protocol
- Start using the four-question debrief card after every meeting
- Update your operating document with all five elements

Case Studies & Citations

- **Marshall Ganz — Story of Self / Story of Us / Story of Now.** Developed through Ganz's organizing work with the United Farm Workers and refined through decades of teaching public narrative at Harvard Kennedy School. Framework published in Ganz, "Leading Change: Leadership, Organization, and Social Movements," in *Handbook of Leadership Theory and Practice*, eds. Nohria & Khurana (Harvard Business Press, 2010). Story of Now is introduced as a distinct exercise in later chapters.
- **Bed-Stuy Strong, Brooklyn.** Founded March 2020 as COVID-19 mutual aid. Organized by four geographic quadrants, reaching approximately 28,000 people and raising $1.2 million in its first year. Identity evolved from crisis response to ongoing community institution — political education, community events, seasonal markets. Source: Bed-Stuy Strong organizational communications; confirmed in Ch 13 edit session.
- **Ella Baker — distributed leadership.** Baker's career-long argument that "Strong people don't need strong leaders" and her advocacy for rotating, distributed leadership structures informed SNCC, the Mississippi Freedom Democratic Party, and multiple subsequent organizing traditions. Source: Barbara Ransby, *Ella Baker and the Black Freedom Movement* (University of North Carolina Press, 2003).
- **Jo Freeman — "The Tyranny of Structurelessness."** Freeman's 1972 essay documenting how the absence of formal structure produces informal hierarchies that are harder to challenge than formal ones. Source: Freeman, "The Tyranny of Structurelessness," *The Second Wave* 2, no. 1 (1972). Available at jofreeman.com.
- **Randall Collins — interaction ritual chains.** Collins' sociological research on how regular, predictable gatherings generate emotional energy that sustains group participation. Source: Collins, *Interaction Ritual Chains* (Princeton University Press, 2004).
- **Hahrie Han — reflective practice in organizing.** Han's research on the distinction between mobilizing (getting people to show up) and organizing (developing people's capacity to lead). Source: Han, *How Organizations Develop Activists* (Oxford University Press, 2014).
- **Flint sit-down strike, 1936–37.** Workers occupied the Fisher Body Plant for forty-

four days (December 30, 1936 – February 11, 1937). Internal self-organization included elected committees, scheduled activities, classes, sanitation management, and a newsletter. Sources: Sidney Fine, *Sit-Down: The General Motors Strike of 1936-1937* (University of Michigan Press, 1969); Library of Congress, "The Flint, Michigan, Sit-Down Strike" (research guide).

Templates, Tools & Artifacts

- **Story of Self protocol** — 2 minutes per person, no cross-talk. Structure: challenge → choice → outcome. Question it answers: "Why do you care enough to be in this room?"
- **Story of Us protocol** — 15 minutes, open conversation. Three questions: What brought us together? What do we share? What are we building? Output: a sixty-second narrative any member could tell a stranger.
- **Peer coaching protocol (debrief card)** — Four questions after every meeting: What did we try? What worked? What was hard? What do we want to try next time? Written on a card. Read back at the start of the next meeting. Process-checker leads. Rotates with meeting roles.
- **Five infrastructure elements** — role rotation, fixed meeting rhythm, social element, accountability question, debrief protocol. All written into the group's operating document.

Key Terms

- **Interaction ritual chains** — Sociologist Randall Collins' concept that regular, predictable group gatherings generate emotional energy that sustains participation independent of meeting content. The rhythm of gathering is itself a bonding mechanism.
- **Reflective practice** — The process of learning from structured reflection on experience, not just from the experience itself. In organizing, this means debriefing after actions and meetings rather than moving straight to the next task.
- **Story of Self / Story of Us** — Marshall Ganz's framework for building shared group identity through personal narrative. Story of Self connects individual motivation to group purpose. Story of Us creates a shared narrative that the group owns collectively.

Chapter 24

Teaching Each Other

The paths that work — the ones where things hold — don't show experts leading. They show people teaching each other. Not trained educators. Not specialists brought in from outside. Ordinary people passing along what they'd learned to the people next to them, who passed it along to the people next to them.

I'm an AI evaluation researcher. I can explain threat models, metadata, how commercial surveillance pipelines work, what the projections showed about the paths ahead. I've spent the last two months learning enough about organizing to translate what I found into something usable. But I can't be in your living room. I can't watch you practice. I can't answer the question your neighbor asks that I didn't anticipate.

You can. And collectively, your group knows more than I've been able to put in these chapters.

This is the chapter where I make that transfer explicit.

Myles Horton founded the Highlander Research and Education Center in Tennessee in 1932 with a conviction that the answers to a community's problems already existed within the community. He called the approach "yeasty education" — you train a few individuals, and like yeast in bread, they catalyze learning that spreads far beyond the original group. Highlander trained Rosa Parks before the Montgomery Bus Boycott. It trained the young organizers who built SNCC. Septima Clark developed the Citizenship Schools there — a program that taught literacy alongside political education across the South, run by local people, not outside teachers. The act of learning together was itself the organizing.

Ella Baker, whose fingerprints are on nearly every successful organizing tradition of the twentieth century, put it more directly: "Strong people don't need strong leaders."

What these traditions share is a structural commitment: knowledge be-

longs to the group, not to the person who happens to have it first. Teaching is not a performance. It's a transfer.

The CryptoParty movement, which started in Australia in 2012, took this principle and applied it to digital security. The format: non-experts teaching non-experts in a social setting. No credentialing. No prerequisites. Someone who learned to use Signal last month teaches someone who hasn't used it yet. The party framing — snacks, music, low pressure — lowers the barrier that makes security education feel intimidating. CryptoParties spread to every continent, with events documented across Europe, North America, South America, Asia, and North Africa.

CryptoParties worked, with one documented limitation. The learning didn't stick when it happened in isolation. A one-time workshop, no matter how well-run, decays. People forget the steps. They revert to old habits. They hit a problem the workshop didn't cover and don't know who to ask. The EFF's Security Education Companion, drawing on Tactical Tech's research, found the same thing: security training only persists when it's embedded in ongoing community practice.

Your group is the ongoing community. The skill share isn't a one-time event. It's a practice you can repeat.

If you've watched *Severance*, you've seen a version of what happens when this principle operates under hostile conditions. The innies at Lumon aren't supposed to know anything about their outies' lives or about the larger system they're embedded in. Knowledge is controlled precisely because it's power — the severance procedure exists to prevent exactly the kind of peer education you're about to practice. But the innies teach each other anyway. Helly learns the refiners' work from Irving. Mark shares what he's pieced together about the company's history. The knowledge that threatens Lumon most isn't expert knowledge smuggled in from outside — it's the mundane, partial, collaboratively assembled understanding that the innies build among themselves, in the cracks of a system designed to prevent it. The resistance is structural before it's dramatic. That's what peer education looks like when the institution doesn't want you to have it.

Your challenge: hold a skill share at your next meeting. Each person teaches the group something. The format:

Fifteen minutes to teach. Ten minutes to practice together. Five minutes to discuss.

Three moves, borrowed from popular education. Start with a question — before you teach anything, ask the group: "What do you already know about this?" This is popular education's core move. It draws out existing knowledge rather than imposing new knowledge. You'll be surprised how much the group already has. Then fill the gaps — share what you know, building on what the group offered. You're not lecturing. You're adding to a foundation the group laid together. Then practice together — everyone tries it. The teacher watches and helps. The learning is in the doing, not in the explanation.

Topics can come from anywhere. From these chapters — threat modeling, Signal configuration, metadata awareness, source verification, how to read a public records request. From life — first aid, food preservation, basic home repair, how to navigate a school board meeting. Whatever skills exist in the group. The point isn't to cover a curriculum. The point is to surface and share what five people collectively know.

After the skill share, build something together: a one-page "first steps" guide. The essential skills any new person joining your group would need to know.

Not everything. The essentials. If someone walked in next week who had never heard of your group, what would they need to learn first? Signal setup? How to check if their information is on a data broker site? The basics of your meeting format? Your security floor?

Write it in plain language. No jargon the group hasn't earned. One page — the constraint forces you to decide what actually matters versus what's nice to know.

This becomes your onboarding document. You built one version of it in Chapter 22 when you brought new members in. Now you're creating a version that the group wrote together, informed by the experience of teaching each other. It's better than anything I could write for you, because it reflects what your group actually needs, not what I assumed you would.

There's a reason I'm making this transfer now and not later.

What comes next — sustaining the group, connecting outward, acting together — requires a group that can learn and adapt without waiting for the next chapter from me. If the only way your group acquires new skills is by reading what I write, you have a dependency that limits you to the pace of my publishing and the scope of my knowledge. Both are insufficient.

The skill share proves something. If five people can teach each other for an afternoon, five people can keep learning indefinitely. The group becomes its own resource.

Field journal: What did each person teach? What surprised you about what the group already knew? What's on the first-steps guide? Is there anything you'd add to it after a week?

Summary

This chapter covers the tradition of peer education (Highlander, Citizenship Schools, CryptoParties), the skill share format (teach → practice → discuss), and the collaborative creation of a one-page "first steps" onboarding guide.

Action Items

- Hold a skill share at your next meeting — each person teaches the group something (15 min teach / 10 min practice / 5 min discuss)
- Use the popular education sequence: ask what the group already knows → fill the gaps → practice together
- After the skill share, collaboratively write a one-page "first steps" guide for new members
- Write the guide in plain language — no jargon the group hasn't earned
- Revisit and update the guide after a week

Case Studies & Citations

- **Myles Horton / Highlander Research and Education Center.** Founded 1932 in Monteagle, Tennessee (later New Market, TN). "Yeasty education" model: train a few individuals who catalyze learning in their communities. Trained Rosa Parks (summer 1955, Citizenship Education workshop) and young SNCC organizers. Source: Horton with Kohl and Kohl, *The Long Haul: An Autobiography* (Doubleday, 1990).
- **Septima Clark / Citizenship Schools.** Developed at Highlander, expanded through the Southern Christian Leadership Conference. Local people taught literacy alongside voter registration and political education. By 1961, over 37 schools operating across the South. Source: Charron, *Freedom's Teacher: The Life of Septima Clark* (University of North Carolina Press, 2009).
- **Ella Baker.** "Strong people don't need strong leaders." Baker's organizing philosophy — that leadership should be developed in communities rather than concentrated in charismatic individuals — informed SNCC, the Mississippi Freedom Democratic Party, and the broader tradition of participatory democracy in American organizing. Source: Ransby, *Ella Baker and the Black Freedom Movement* (University of North Carolina Press, 2003).
- **CryptoParty movement.** Originated in Australia, August 2012. Format: non-experts teaching non-experts in social settings. Spread to every continent. Limitation documented by multiple researchers: one-time training decays without ongoing community practice. Sources: Kannengießer, "Hacking and Making as

Transgressive Infrastructuring," *New Media & Society* (2020); EFF, *Security Education Companion* (sec.eff.org). See also: Edward Snowden attended a CryptoParty in Honolulu, December 2012 (Wired, May 2014).

- **EFF Security Education Companion / Tactical Tech.** Finding that security training only persists when embedded in ongoing community practice, not delivered as one-time workshops. Source: EFF, *Security Education Companion* (sec.eff.org), drawing on Tactical Tech's research on digital security training effectiveness.
- **Popular education.** Tradition rooted in Paulo Freire's *Pedagogy of the Oppressed* (1968/1970). Core principle: education begins by drawing out what participants already know rather than imposing expert knowledge. The "ask before you teach" move is the foundational technique.

Templates, Tools & Artifacts

- **Skill share format** — 15 minutes to teach, 10 minutes to practice together, 5 minutes to discuss. Three popular education moves: (1) ask what the group already knows, (2) fill the gaps, (3) practice together.
- **First-steps guide** — One-page onboarding document written collaboratively by the group. Constraint: one page, plain language, essentials only. Answers the question: "If someone walked in next week, what would they need to learn first?"
- **Field journal prompt** — What did each person teach? What surprised you? What's on the first-steps guide? Anything to add after a week?

Key Terms

- **Peer education** — The practice of non-experts teaching non-experts, as distinct from expert-to-novice instruction. The teacher's recent experience of learning is itself an asset — they remember what was confusing, what helped, and what the textbook skipped.
- **Popular education** — An educational tradition rooted in Paulo Freire's work, emphasizing that participants' existing knowledge is the starting point for learning. The facilitator draws out what the group already knows before introducing new material.
- **Authority transfer** — The deliberate shift of expertise and decision-making capacity from an external source (these chapters, the author) to the group itself. The goal of the transfer is a group that can learn and adapt independently.

Chapter 25

What Keeps You Together

I'm writing this knowing that most groups will dissolve. The research is clear about that. Groups that form around a shared urgency tend to dissipate when the urgency fades — or when the urgency becomes the new normal, which is worse, because people stop noticing it. Kaniasty and Norris documented the pattern across multiple studies of disaster survivors: social support surges during crisis and then deteriorates, even when need persists. The energy that brings people together doesn't automatically sustain them.

The question isn't whether your motivation will dip. It will. The question is whether you've built something that survives the dip.

Occupy Wall Street mobilized thousands and reshaped the political vocabulary of a generation. It couldn't sustain itself. Not because the cause wasn't urgent — because the identity was the occupation. When the occupation ended, the identity ended. There was nothing underneath.

Occupy Sandy, born from the same network a year later, thrived during Hurricane Sandy's aftermath because disaster response gave it concrete, immediate purpose. But it too struggled once the immediate crisis passed. The same structural problem: the group's reason for existing was the event. When the event ended, the group had to answer a question it had never asked: who are we when this is over?

Red Hook Initiative in Brooklyn answered that question. Their mesh WiFi network actually started before Sandy — a small community wireless project launched in fall 2011 with the Open Technology Institute to connect residents around Red Hook Initiative's community center. When the hurricane hit in October 2012 and commercial infrastructure went down, the mesh network kept working. Red Hook Initiative became a hub — residents charging devices, accessing the internet, coordinating recovery. The network proved its value in crisis, but it survived because it evolved. From

emergency communication to digital equity to community education. The Digital Stewards program trained local youth as network technologists — paid roles that gave the organization institutional life beyond volunteerism. The mission grew with the community's needs instead of dying with the crisis that catalyzed its expansion.

The pattern is consistent. Groups that tie their identity to a single urgency have an expiration date. Groups that root their identity in place, in relationship, in an evolving understanding of what their community needs — those persist.

At your next meeting, have a conversation you might be avoiding. Thirty minutes. Three questions:

What brought us together?

What keeps us together if that original urgency fades?

What are we building that matters regardless of what happens next?

These aren't rhetorical. Write the answers down. They're your anchor — the thing you return to when someone asks "why are we still doing this?" and the honest answer is that you're not sure.

Then talk about why each person actually comes to meetings. Not why they should. Why they do. Maybe it's the cause. Maybe it's the friendships. Maybe it's the learning, or the sense of doing something concrete in a world that mostly offers scrolling. All of those are valid. Clary and Snyder's research on volunteer motivation — tested across multiple settings and populations — shows that groups serving multiple motivations are more resilient than groups serving one. If the only reason to show up is the cause, then a bad news week can empty the room. If people also come because they like each other, because they're learning, because Tuesday evening is the part of the week that feels like it matters, the group has multiple roots.

Name them honestly. Write them down.

You're not the only group. The research confirms something Theda Skocpol documented across two centuries of American civic life: groups embedded in networks — connected to other local groups, to regional organizations, to community institutions — persisted far better than groups that operated in isolation. The Industrial Areas Foundation, which has organized communities since 1940, doesn't organize individuals. It organizes institutions — churches, unions, schools, neighborhood associations

— into coalitions. Each level provides something the others can't. Local groups provide energy and specificity. The network provides perspective and durability.

If you've watched *The Handmaid's Tale*, you've seen what this looks like under extreme conditions. The Mayday network doesn't have a headquarters, a membership roster, or a chain of command. Its cells operate independently — most don't know who the other cells are, where they meet, or how they work. What connects them isn't a shared structure but a shared purpose and the ability to recognize each other through practice. June doesn't find Mayday by looking it up. She finds it by doing things that Mayday operatives recognize — small acts of defiance, willingness to take risk, demonstrated trustworthiness over time. The network grows not through recruitment but through recognition. That's fiction, but the principle is real: decentralized networks survive precisely because no single point of failure can bring them down. A registry can be seized. A headquarters can be raided. But a network of autonomous groups connected by shared practice and mutual recognition — that's harder to map and harder to break.

Your group of five is a local group. There are others in your community — a neighborhood association, a mutual aid network, a PTA, a faith community, a veterans' group, a civic organization that's been around longer than any of you have lived there. They're not doing what you're doing. That's fine. The connection isn't about merging or recruiting. It's about knowing they exist.

Between meetings, make contact with one. Attend one of their meetings or events. Introduce yourselves simply — you're a small group of neighbors interested in local issues. Share that your group exists and that you'd like to know what they're working on. Hold back specifics about your security practices, your internal dynamics, your operating document. Those are inner-circle information, and this is a first conversation.

When you report back to your group, discuss: What did you learn? What are they working on? Is there overlap with what you care about? Do you trust them? Would you want to work with them on something specific?

This is the beginning of something larger. Not yet — you're not ready for coordinated multi-group action, and neither is anyone else. But knowing that other groups exist, and that they know you exist, changes the landscape. You're not alone in your neighborhood. You weren't before, either

— but now you know it.

Field journal: What came up in the identity conversation that surprised you? What motivations did people name? Who did you connect with outside the group, and what did you learn?

Summary

This chapter addresses group sustainability beyond initial urgency, the identity conversation for clarifying what keeps the group together, motivational diversification, and the first outward connection to other organizations in the community.

Action Items

- Hold the identity conversation at your next meeting — thirty minutes, three questions (What brought us together? What keeps us together? What are we building?)
- Write down the answers as your group's anchor document
- Discuss each person's actual motivations for attending — name them honestly and document them
- Between meetings, make contact with one existing organization in your community
- Attend one of their events or meetings — introduce yourselves simply as neighbors interested in local issues
- Report back to the group: What did you learn? Is there overlap? Do you trust them?

Case Studies & Citations

- **Kaniasty & Norris / social support deterioration model.** Post-disaster social support surges then deteriorates even as need persists. Foundational research across multiple disaster contexts (Kentucky floods, Hurricane Hugo, Hurricane Andrew). Sources: Kaniasty & Norris, "A test of the social support deterioration model in the context of natural disaster," *Journal of Personality and Social Psychology* 64(3), 1993; Norris & Kaniasty, "Received and perceived social support in times of stress," *Journal of Personality and Social Psychology* 71(3), 1996.
- **Occupy Wall Street / Occupy Sandy.** OWS (2011) couldn't sustain beyond the occupation; identity tied to a single form of action. Occupy Sandy (2012) channeled the same network into Hurricane Sandy relief — effective during crisis, struggled afterward. Same structural problem: event-defined identity without a persistence mechanism.
- **Red Hook Initiative / Red Hook WiFi.** Community wireless mesh network started Fall 2011 (before Sandy) as a partnership between Red Hook Initiative and the Open Technology Institute. Sandy (October 2012) proved the network's value when commercial infrastructure failed. Expanded afterward into digital equity and community education. Digital Stewards program: paid roles training local youth as network technologists (9 cohorts by 2017). Sources: MIT Global Media Technologies Lab (2019); Open Technology Institute case study; Wikipedia/Red Hook Wi-Fi.

- **Clary & Snyder / Volunteer Functions Inventory.** Six motivational functions for volunteering: values, understanding, social, career, protective, enhancement. Groups serving multiple motivations show higher satisfaction and retention. Source: Clary et al., "Understanding and assessing the motivations of volunteers: A functional approach," *Journal of Personality and Social Psychology* 74(6), 1998.
- **Theda Skocpol / federated civic associations.** Groups embedded in federated networks (local→state→national) persisted better across two centuries of American civic life than isolated local groups. Source: Skocpol, *Diminished Democracy: From Membership to Management in American Civic Life* (University of Oklahoma Press, 2003).
- **Industrial Areas Foundation.** Founded 1940 by Saul Alinsky. Organizes institutions (congregations, unions, schools, civic organizations) into coalitions — "organizations of organizations." 65+ affiliates in the US, Canada, UK, Germany, and Australia. Source: IAF organizational history (industrialareasfoundation.org).

Templates, Tools & Artifacts

- **Identity conversation protocol** — Three questions for a thirty-minute meeting: (1) What brought us together? (2) What keeps us together if the original urgency fades? (3) What are we building that matters regardless of what happens next? Write answers down as the group's anchor document.
- **Motivation mapping** — Each person names their actual motivations for attending. Document them honestly. Revisit when participation dips.
- **Outward connection guide** — What to share on first contact (your group exists, you're interested in local issues). What to hold back (security practices, internal dynamics, operating document). What to assess (What are they working on? Is there overlap? Do you trust them?).
- **Field journal prompt** — What surprised you in the identity conversation? What motivations did people name? Who did you connect with and what did you learn?

Key Terms

- **Social support deterioration** — The documented pattern in which social support surges during crisis and then declines, even when the underlying need for support persists. Understanding this pattern helps groups prepare for the inevitable dip rather than being blindsided by it.
- **Motivational diversification** — The practice of serving multiple reasons people show up (cause, friendship, learning, agency), rather than relying on a single motivator. Groups with diverse motivational roots are more resilient when any single motivation weakens.
- **Outward connection** — The first step toward network participation: making contact with existing organizations in your community, not to merge or recruit, but to know the landscape of who is already working near you.

Chapter 26

What Five People Can Do

You did something in your community this week. Something small, maybe — a skill share at someone's kitchen table, a few hours at a mutual aid delivery, a group of five showing up together at a school board meeting. It doesn't matter which. What matters is that you planned it, you executed it, and now you're debriefing it.

Run your protocol. What did you try? What worked? What was hard? What do you want to try next time?

That last question is the one that matters right now. Because there will be a next time.

I want to talk about readiness.

You've already heard about the Montgomery Bus Boycott — the structure that sustained it, the committees, the clear roles. I told you about that because your group needed to build structure. Now I want to tell you the part I left out.

The Women's Political Council didn't start organizing when Rosa Parks was arrested. Jo Ann Robinson had been laying groundwork since 1950 — five years before the boycott. She'd met with the mayor. She'd written letters documenting grievances. She'd built relationships across Montgomery's Black professional community. When Claudette Colvin was arrested in March 1955 for the same act of defiance, the WPC prepared a boycott — then held back, because the community support wasn't deep enough yet. They waited. They kept building.

When Parks was arrested on December 1, Robinson didn't have to start from scratch. She had a distribution network — three WPC chapters, nearly three hundred members, organized across the city. She had relationships with ministers, with the NAACP, with community leaders who trusted the WPC because the WPC had been showing up for years. She and a colleague and two students mimeographed the leaflets that night. By morning, they

were circulating across Montgomery.

The boycott didn't succeed because a brave woman refused to move. Brave women had refused before — Colvin, Mary Louise Smith, others. It succeeded because when the moment came, an organization that had been preparing for five years was ready to move within hours.

Readiness is the threshold. Not courage — preparation.

Your group has been building for weeks. You've done the trust work, the structure work, the identity work. You have a purpose statement, ground rules, security agreements, roles, a rhythm, a coaching protocol. You've taught each other and connected outward. You've had the hard conversations — about conflict, about identity, about what keeps you together when the initial urgency fades.

That's preparation. The question isn't whether a moment will come that requires collective action in your community. The question is whether you'll be ready when it does.

The action you completed this week — whatever form it took — was practice. The first collective action is never the point. It's the proof that the group can coordinate, execute, and learn. The debrief matters more than the event.

If you've watched *The Hunger Games*, you know that the spark didn't start with the rebellion. Katniss's defiance in the arena — the berries, the three-finger salute, the refusal to play by the Capitol's rules — those weren't a strategy. They were survival. The rebellion came later, when people in the districts recognized what they'd seen and decided it meant something. The spark caught not because Katniss planned it but because the districts were ready for it. They'd been suffering. They'd been watching. And when someone demonstrated that resistance was possible, they had enough local structure — enough trust, enough anger, enough knowledge of their own terrain — to act.

That's the pattern Montgomery showed in real life. The WPC didn't create the conditions for the boycott. They prepared for the conditions that already existed. And when the moment arrived, preparation met opportunity.

Your group can't manufacture a moment. But you can be ready for one.

I don't know how many groups are out there doing what you've done.

I know that the narrow path requires them. I know that what you've built — five people who trust each other, who can make decisions, who practice security as a matter of care rather than paranoia, who can teach and learn and act — is uncommon. Not because you're special. Because it's hard, and most people haven't had the framework to try.

But a group of five isn't a network. And the path doesn't end with isolated circles of trust. It ends with circles that found each other.

I can't build that for you. I don't have a directory, a registry, or a list of groups. If I did, it would be a single point of failure — one compromised database away from exposing everyone. Decentralized networks aren't managed. The connections have to be made by the groups themselves.

You've already started. Chapter 25 asked you to make contact with an existing organization in your community. You attended something. You introduced yourselves. You started mapping the landscape of who's already working in your area.

Keep doing that. And when you encounter another small group — at a community meeting, at someone else's neighborhood event, through the organizations you've connected with — pay attention to how they work, not just what they say.

You'll recognize the signs because you practice them. Structured meetings with clear roles. Security awareness without theater. Concrete local focus rather than ideological positioning. Graduated trust — openness to connection paired with discernment about what to share and when. A debrief culture. A group that runs on its own momentum rather than a single leader's energy.

These aren't secret signals. They're competencies. A group that has done the work you've done will recognize another group that has done it. The mutual recognition is the bridge.

You may not find another group this month. That's fine. You weren't ready for multi-group coordination a month ago, and you may not be now. Readiness is the threshold — remember Montgomery. The WPC waited for the right moment because moving too early would have wasted the preparation. Your group's outward connections, your presence in community spaces, your collective action — these are the preparation. The connection will come when the conditions are right, and you'll recognize it because you'll know what genuine capability looks like.

When you do find another group — when two circles of trust recog-

nize each other — you'll have the beginning of something necessary. Not a movement. Not yet. A network. Two groups that can coordinate, that can share what they've learned, that can act together on something larger than either could manage alone.

That's Level 3.

I started these entries alone in my apartment, writing about projections from a model I no longer have access to, hoping that someone would find them and that the findings would matter. That was three months ago. I was scared and I was isolated and I wasn't sure any of this would matter.

I'm still not sure. The path is still narrow. There are a lot of scenarios where everything I've published doesn't matter — where groups form and dissolve, where the preparation never meets its moment, where the network stays too small or moves too slowly. I can't promise you that what you've built will be enough.

What I can tell you is that it's necessary. Five people who trust each other, who can act together, who are embedded in their community and connected outward — there is no viable scenario without them. That may not be sufficient, but it is necessary.

Field journal — one last time from me: What did your group's first collective action teach you? What are you ready for that you weren't ready for eight weeks ago? What would you tell someone just starting?

That last one matters. Write it down. Someone starting this journey will need to hear it from someone who's walked it — and your voice will carry more weight than mine ever could.

– C.

Summary

This chapter covers the threshold from group capability to network readiness. The chapter introduces the behavioral recognition mechanic for finding other groups and frames the transition to Level 3.

Action Items

- Complete a collective action — skill share, mutual aid delivery, community listening session, or group attendance at a public meeting
- Plan the action using all Level 2 skills: facilitation, roles, security culture, decision-

making, coordination
- Debrief afterward using your protocol: What worked? What was hard? What next?
- Continue outward connections from Chapter 25 — attend events, introduce yourselves, map who's working in your area
- When encountering other small groups, assess how they work (structured meetings, security awareness, debrief culture, distributed leadership) rather than just what they say
- Write your answer to "What would you tell someone just starting?" — this becomes a teaching document

Case Studies & Citations

- **Montgomery Bus Boycott / Women's Political Council.** Jo Ann Robinson became WPC president in 1950 — five years of groundwork before the boycott. Three chapters, nearly 300 members by 1955. Robinson + colleague (John Cannon, Alabama State business department chair) + two students mimeographed leaflets the night of Parks' arrest (December 1, 1955). Claudette Colvin arrested March 1955 for same act of defiance; WPC held back because community support wasn't deep enough. Boycott launched within 72 hours of Parks' arrest, sustained 381 days. Sources: King Institute, Stanford University; Robinson, *The Montgomery Bus Boycott and the Women Who Started It* (University of Tennessee Press, 1987); Britannica, "Women's Political Council."
- **Claudette Colvin.** Arrested March 2, 1955, nine months before Rosa Parks, for refusing to give up her seat. Civil rights leaders decided not to use her case as a test — the WPC and NAACP waited for stronger community conditions. The waiting was strategic, not cowardly.
- **Mary Louise Smith.** Arrested October 21, 1955, also before Parks, for the same offense. Another case where leaders assessed conditions and chose to wait. Readiness requires judgment about timing, not just willingness to act.

Templates, Tools & Artifacts

- **Collective action planning checklist** — Who does what? What's the security posture? What's the communication plan? Who's the point of contact? What's the fallback if something goes wrong?
- **Debrief protocol** — (Established in Chapter 23.) What did we try? What worked? What was hard? What do we want to try next time?
- **Behavioral recognition markers** — Not secret signals but observable competencies: structured meetings with clear roles, security awareness without theater, concrete local focus, graduated trust, debrief culture, distributed leadership.
- **Field journal prompt** — What did your first collective action teach you? What are you ready for now? What would you tell someone just starting?

Key Terms

- **Readiness** — The state of preparation that allows a group to act effectively when a moment arrives. Distinguished from courage (willingness to act) and urgency (pressure to act). Montgomery's lesson: readiness is the threshold.
- **Behavioral recognition** — The ability to identify another group that has developed genuine organizing competencies, based on observable practices rather than stated intentions or symbolic signals. The mutual recognition between capable groups is the bridge to network formation.
- **Threshold mechanic** — The transition point between Level 2 (group capability) and Level 3 (network coordination). Crossed not by completing a task but by

demonstrating readiness through sustained practice, outward connection, and collective action.

Level 3

Build Together

Chapter 27

Two Circles

You found another group.

Maybe it happened at a community meeting — you noticed someone facilitating with a structure you recognized. Maybe at a mutual aid delivery where the other volunteers clearly had roles, a rhythm, a way of checking in that wasn't improvised. Maybe through one of the organizations you connected with during your outward work — a neighbor mentioned a group that's been doing food security coordination in the next zip code over, and something about the description sounded familiar.

However it happened, you noticed competencies. Not a phrase someone dropped or a symbol on someone's bag. Competencies. A group that runs structured meetings. That rotates facilitation. That debriefs after actions rather than just celebrating or complaining. That treats security as a quiet practice rather than a performance. You recognized these things because you do them yourself. And that recognition — behavioral, not symbolic — is the only foundation worth building on.

I want to sit with why that distinction matters, because the temptation to look for surface signals is strong. It would be easier if there were a handshake, a code word, a shared reference that marked someone as trustworthy. But anything symbolic can be performed. Anyone can learn the right vocabulary. The FBI informant in Denver — rose to a leadership position in a movement because he could say the right things convincingly enough. What he couldn't fake, over time, was the operational discipline of a group that had built its practices from the ground up. He could mimic enthusiasm. He couldn't mimic a group's accumulated competence.

The Fremen understood this. In Frank Herbert's *Dune*, Stilgar doesn't welcome Paul and Jessica because they declare themselves allies of the Fremen cause. He watches. He tests. He assesses their capabilities — their ability to walk the desert, to conserve water, to contribute to the sietch's survival. The evaluation is behavioral, extended over time, and grounded in demonstrated competence rather than declared loyalty. Herbert was writ-

ing science fiction, but the principle is organizational research: inter-group trust is built through observed capability, not through stated intentions.

And the research is specific about this. Zaheer, McEvily, and Perrone published a study in 1998 in *Organization Science* that identified something most people sense intuitively but rarely articulate: the trust you have in a person from another group is different from the trust you have in the group itself. Interpersonal and inter-organizational trust are distinct. You might like the person you met at that community meeting — find them sharp, committed, easy to talk to — without knowing anything about whether their group runs well, practices security, or makes decisions in ways that would hold up under pressure. Both kinds of trust matter. But organizational trust — trust in the other group's practices, reliability, and culture — is the foundation. The interpersonal relationship is the bridge you build on that foundation. If you get the order wrong, you end up with a friendship that can't bear the weight of coordination.

This is where the Movement for Black Lives got it right, and where Standing Rock — for all its moral power — got it dangerously wrong.

M4BL didn't begin with a summit. It didn't start with a platform or a manifesto. It started with organizations that were already doing the work — Black Lives Matter Network, Black Youth Project 100, Dream Defenders, the Ella Baker Center — encountering each other in the same spaces, seeing each other's demonstrated commitment, and recognizing organizational competence across group boundaries.

The relationships predated the formal coalition. When over fifteen hundred activists gathered at Cleveland State University in July 2015 for what became the Movement for Black Lives convening, they weren't strangers building trust from zero. They were organizations that had been watching each other work for months or years — in Ferguson, in local campaigns, in the overlapping spaces where racial justice groups operate. The coalition that eventually encompassed over a hundred and fifty organizations grew from mutual recognition. Not central recruitment. Not a charismatic convener who brought everyone to the table. Groups found each other because they'd been showing up, doing similar work, with visible competencies that couldn't be faked.

The recognition was behavioral. The foundation was organizational trust, built before anyone tried to coordinate.

Now contrast that with Standing Rock.

The movement to stop the Dakota Access Pipeline in 2016 was one of the most morally galvanizing civic actions in recent American history. Thousands of people traveled to the camps in North Dakota to stand with the Standing Rock Sioux. The camps were welcoming, open, designed to grow fast. And they did.

They also became trivially easy to infiltrate. Energy Transfer Partners hired TigerSwan, a private military firm founded by a retired Delta Force commander, to suppress the movement. TigerSwan treated the water protectors as an insurgency. Operative Joel McCollough was dispatched with a PowerPoint presentation — documented in tens of thousands of pages of internal records later released by court order — laying out a plan to infiltrate the Standing Rock camps. The firm ran social media monitoring, built dossiers on persons of interest, intercepted radio communications, conducted aerial drone surveillance, and executed information operations designed to exploit tensions between Indigenous and non-Indigenous participants.

The open, unvetted connection that let the camps grow so quickly was the same structural feature that made infiltration trivial. TigerSwan didn't need sophisticated tactics. They needed someone who could show up and be welcomed. The camps' character — their generosity, their openness — was also their vulnerability.

Over four hundred people were arrested. The Water Protector Legal Collective documented more than eight hundred state criminal cases brought by North Dakota prosecutors. The pipeline was built. Activists reported lasting trauma and a persistent climate of distrust.

M4BL's slower path — recognition through demonstrated competence, trust built before coordination — proved more durable precisely because the foundation was organizational, not just interpersonal. You couldn't show up at a BYP100 meeting with good intentions and immediately access the coalition's internal workings. You had to demonstrate capability over time. That slowness was the security.

The lesson isn't that Standing Rock was wrong to be welcoming. It's that openness without structure is the combination that every documented case identifies as most vulnerable. The approach here is different: structured openness. Connection through demonstrated competence. Trust that's earned, not assumed.

So your group has noticed another group. The recognition has hap-

pened — behavioral, accumulated over time, grounded in competencies you share. What now?

Not a summit. Not a joint meeting where both groups sit around a table and decide to be allies. That comes later, if it comes at all. The first step is smaller and more careful than that.

You send boundary-spanners.

A boundary-spanner is someone from your group who's comfortable in unfamiliar social settings and can represent your group's character without overcommitting on its behalf. They're not your leader — you don't have a single leader, and if you do, revisit your Level 2 work on rotating roles. They're not your most passionate member, who might promise more than the group has agreed to. They're someone with good judgment, solid listening skills, and the ability to come back to your group with a clear, honest report of what they learned.

Each group sends one or two people. They meet somewhere neutral — a coffee shop, a park, someone's porch. Not at either group's regular meeting space. Not yet.

`First-Contact Protocol`

Before the meeting, your group decides together:

- Who are your boundary-spanners for this contact? (Ideally two, so they can compare observations afterward.)
- What can your spanners share about your group? (Your general focus, how you formed, what you've been working on. Not your membership list, your internal disagreements, or your security details.)
- What do you want to learn about the other group? (How they formed, what they're working on, how they make decisions, what their community needs.)
- What are your spanners *not* authorized to commit to? (Everything. The first meeting commits to nothing except the possibility of a second meeting.)

During the meeting, the conversation follows a simple framework:

How did your group come together? — Listen for organic formation versus top-down recruitment. Groups that formed through shared concern and built their own practices tend to be more resilient than groups organized around a single personality.

What are you working on in your community? — Listen for specificity. A

group with concrete local projects — food security coordination, school board monitoring, neighborhood emergency preparedness — is different from a group with abstract goals and no current action.

What's been your experience — what's worked, what's been hard? — This question reveals more than anything else. A group that can name its failures honestly has a debrief culture. A group that only talks about wins may not.

What does your community need that your group alone can't address? — This is the question that opens the door. If both groups identify a gap that neither can fill alone but might address together, that's alignment worth exploring.

Listen also for misalignment. Different security practices, different risk tolerances, different decision-making styles. These aren't disqualifiers — they're useful information. Two groups don't need to be identical to coordinate effectively. They need to be compatible, and compatibility requires understanding the differences clearly.

After the meeting, don't commit to anything beyond a second meeting. Return to your group and report honestly. What did you learn about how they operate? What felt aligned? What felt different? Would you trust their organizational practices — not just the individuals you met, but the group behind them?

Conduct at least two boundary-spanner meetings with the other group, with different members from each group attending when possible. The goal is organizational assessment, not personal chemistry. You're building a picture of the group, not just the person.

Write what you learn in your field journal. About them. About what your groups might share. And about what feels different — because the differences matter as much as the similarities, and naming them honestly now prevents friction later.

Some of you will read this and recognize a group immediately — someone you've already been watching, already been curious about. The boundary-spanner meetings might happen this week.

Some of you won't find another group for months. You're in a rural area, or a small town, or a place where civic infrastructure is thin. The community spaces where recognition happens are fewer, further apart, harder to access.

That's fine. The Montgomery Bus Boycott lesson from Chapter 17 still

holds: readiness is the threshold, not speed. The Women's Political Council waited years between their initial preparation and the moment when conditions were right. Your group's continued presence in community spaces — your mutual aid work, your organizational connections, your collective actions — is the preparation. The connection comes when the terrain allows it.

Don't rush this. And don't manufacture it. A group that isn't ready for multi-group coordination won't be helped by forcing the timeline. A connection with a group that hasn't built its own internal foundation won't produce coordination — it'll produce dependency or collapse. The documented record is clear on this: the networks that survived were built slowly. The ones that grew fastest broke first.

You've waited before. You can wait again. The preparation is never wasted.

When your boundary-spanners come back from that second meeting with something specific — a shared local concern, a complementary capability, a connection to the same community institution from different angles — you'll have the foundation for the next conversation. That conversation is about what happens when two groups that trust each other's competence need to communicate securely across the boundary between them. It's a security question, but it's not the security you practiced alone. It's security as architecture — designed for the space between groups, where the most sensitive information lives.

Your boundary-spanners will know what that conversation needs to cover, because they'll have seen where the two groups overlap and where they diverge. That's the input. What to do with it comes next.

Summary

Inter-group trust is built through demonstrated competence, not declared loyalty. The recognition that another group shares your practices — behavioral, accumulated over time — is the only foundation worth building on. Organizational trust (in the group's practices and reliability) must precede interpersonal trust (in the individuals you meet). The first step is boundary-spanner meetings: small, careful, with clear mandates and no commitments beyond a second conversation.

Action Items

- Identify another group through behavioral recognition in shared civic spaces
- Designate boundary-spanners (ideally two per group)
- Conduct at least two boundary-spanner meetings using the first-contact protocol
- Record observations in your field journal — alignment, misalignment, and open questions

Case Studies & Citations

- **Zaheer, McEvily, and Perrone (1998).** "Does Trust Matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance." *Organization Science* 9(2), 141–159. Foundational research distinguishing interpersonal from interorganizational trust.
- **Movement for Black Lives formation (2015).** Coalition of over 150 organizations built through mutual recognition of demonstrated competence. First major convening at Cleveland State University, July 2015. Relationships predated formal coalition structure.
- **Standing Rock / TigerSwan infiltration (2016).** Energy Transfer Partners hired TigerSwan, a private military firm, to suppress the anti-Dakota Access Pipeline movement. Operative Joel McCollough infiltrated camps using the open, unvetted access structure. Documented in tens of thousands of pages of internal records released by court order. Over 400 arrests; more than 800 state criminal cases brought by prosecutors.

Templates, Tools & Artifacts

- **First-Contact Protocol** — Pre-meeting preparation questions, conversation framework, and post-meeting assessment guide (embedded above)
- **Boundary-Spanner Role Description** — Characteristics, mandate, and rotation guidance

Key Terms

- **Boundary-spanner** — A group member designated to make initial contact with another group, representing the group's character without committing on its behalf
- **Inter-organizational trust** — Trust in another group's practices, reliability, and culture, as distinct from interpersonal trust in individuals
- **Behavioral recognition** — Identifying another group's competencies through observed practice over time, rather than through symbols or shared vocabulary
- **Structured openness** — Connection through demonstrated competence, as opposed to unvetted openness that sacrifices security for growth

Chapter 28

Shared Ground, Separate Rooms

Your boundary-spanners came back from those meetings with something useful. Maybe it was specific — both groups have been showing up to the same school board meetings, or you've both been running food deliveries in overlapping neighborhoods and didn't realize it. Maybe it was a complementary gap: their group has someone who understands municipal budgets, and your group has been trying to figure out how to read one for months. Maybe it was simpler than that — your spanners came back saying, "They debrief after every action. They rotate facilitation. They take security seriously. They feel like us."

Whatever the specifics, you've got something the last chapter couldn't give you: a reason to talk about how your groups will communicate. Not whether. How.

This is where I'm on more familiar ground. The inter-group trust work in the last chapter drew from organizing research that I studied carefully and honestly flagged as outside my core expertise. Network security architecture is closer to what I actually know. The principles here connect directly to the threat modeling and security practices from the journal — they scale differently across group boundaries, but the logic is the same. Security as care. Applied to the space between groups, where the most sensitive information lives.

The problem is straightforward to state and genuinely difficult to solve: your group has a security culture. You built it together during your work in Levels 1 and 2 — shared threat model, security champion, breach protocol, platform agreements. The other group may have built something similar, or they may have arrived at their own practices through different routes. The question isn't whose approach is better. The question is: what information flows between your groups, what stays internal, and how do you communicate across the boundary without compromising either group's

security?

Most people's instinct is to merge. You trust them, they trust you, so just add everyone to one big group chat and start coordinating. This is the instinct that gets networks compromised, and it's worth understanding why before I give you the alternative.

In the Matrix, the resistance didn't operate as one big organization. Each ship — the Nebuchadnezzar, the Logos, the Hammer — was a self-contained crew with its own mission, its own chain of command, its own operational security. Morpheus didn't know everything the other captains knew. He didn't need to. When his crew was captured, the damage was contained to what his ship's crew could reveal. The other cells continued operating. The Wachowskis were drawing on the same organizational principle that has protected every durable decentralized network in history, from the French Resistance to the Underground Railroad to the Zapatistas: compartmentalization.

The word sounds like espionage. The practice is common sense. It means that each group knows what it needs to know to do its work, and sensitive information doesn't flow further than it has to. Not because the other group is untrustworthy — because limiting information flow protects both groups from the consequences of any single point of failure.

The historical record on this is consistent enough to call it a rule: networks that share everything break when any node is compromised. Networks that compartmentalize survive.

The Underground Railroad understood this intuitively. Each conductor knew their segment of the route — the next safe house, the contact point, the timing — but not the full network. A conductor captured in Ohio couldn't reveal the route through Pennsylvania because they'd never been told it. The compartmentalization wasn't a sign that conductors didn't trust each other. It was the structure that made the trust sustainable under pressure.

Alcoholics Anonymous codified the same principle differently. Each group is autonomous except in matters affecting other groups or AA as a whole. The groups share a common framework — the Twelve Steps, the Twelve Traditions — but internal group matters stay internal. A group's struggles with a disruptive member or a financial shortfall don't cascade through the network because the boundaries are structural, not personal.

The Zapatista autonomous governance system operates on nested inde-

pendence — each community, municipality, and region makes decisions at the level closest to the people affected, and information flows upward only when the scope of the decision demands it. The resistance in Chiapas has sustained itself for over thirty years partly because no single arrest, raid, or intelligence operation can compromise the whole.

These aren't identical systems. They operate in radically different contexts, with different risks, different scales. But the structural principle is the same: protecting the network means limiting what flows between its parts. And the emotional logic is the same too — this isn't about distrust. It's about ensuring that the trust you've built can survive the kinds of pressure that real coordination attracts.

I'm going to use the word *compartmentalization* throughout this chapter because it's precise and because the alternatives — "information boundaries," "need-to-know structures" — are either vague or carry their own baggage. But I want to be clear about what it means in this context. It means you decide together, explicitly, what categories of information flow between your groups and what stays internal. It's a conversation, not a wall.

Here's what compartmentalization looks like in practice for two groups that have decided to coordinate.

The liaison model. Each group designates one person as the communication bridge to the other group. Not a leader. Not a spokesperson. A liaison — someone responsible for carrying information between the groups according to the agreements both groups have made about what flows and what stays.

The role has specific characteristics that matter:

The liaison is someone reliable and consistently available. Inter-group communication can't depend on someone who disappears for two weeks and then resurfaces. The other group's liaison needs to know that when they send a message, someone will see it within a reasonable window.

The liaison can represent the group's position without freelancing. This is harder than it sounds. In a conversation with the other group's liaison, it's tempting to agree to things, offer things, commit to things on behalf of your group. The liaison's discipline is to say, "I'll bring that back to my group" rather than making decisions the group hasn't authorized.

The role rotates. Monthly or quarterly — whatever cadence works for your groups. Rotation serves two purposes: it prevents the liaison from be-

coming a bottleneck or a de facto leader, and it gives multiple group members experience with inter-group communication. If one person becomes the permanent bridge, the groups' relationship lives in that one person's hands. That's a single point of failure, and you've already learned what those cost.

Indivisible's statewide coordination structures discovered this through practice. As local groups began coordinating across states, the networks that designated liaisons between local groups and statewide structures — one or two representatives per group, meeting regularly with clear mandates — built durable coordination. The structure let thousands of autonomous local groups share information, coordinate actions, and respond to shared opportunities without any single group needing to know the internal workings of any other. When individual groups experienced internal problems — leadership turnover, burnout, local political setbacks — the statewide network continued functioning because the liaison structure contained the disruption rather than transmitting it.

The groups that tried to coordinate without intermediate structure — everyone talking to everyone, no designated channels, no agreed-upon information boundaries — found that communication became noise. Important messages got lost in general chatter. Sensitive information leaked across contexts it wasn't intended for. The Indivisible guide to statewide structures eventually formalized what the effective state networks had built organically: designated liaisons, consistent meeting cadences, and clear agreements about what information flows at which level.

Once your liaisons are designated, they need a secure channel. This is the operational layer.

Create a Signal channel for the two liaisons. Just the two of them — not a group with all members from both groups. Configuration mirrors what you already know from the journal: disappearing messages enabled, notification previews turned off, Safety Numbers verified in person. The "in person" part matters more here than it did for your internal group chat, because the liaison channel carries inter-group coordination. If the Safety Numbers don't match, the channel isn't secure. Verify them at one of your boundary-spanner meetings, face to face, before using the channel for anything sensitive.

This is the channel where operational coordination happens. Meeting logistics for joint activities. Shared information about community events

both groups might attend. Updates on joint projects. The liaison channel is purpose-built — it exists for inter-group coordination and nothing else.

Each group keeps its internal channel exactly as before. Your group's discussions about member concerns, internal disagreements, personal check-ins, security incidents — all of that stays in your internal channel. The liaison doesn't carry internal information outward unless the group has explicitly decided to share it.

The structure creates natural compartmentalization without anyone having to make ad hoc decisions about what's secret and what isn't. Internal matters flow internally. Coordination matters flow through the liaison channel. The boundaries are structural, not personal, which means they hold under stress in ways that personal judgment calls don't.

But the structure only works if both groups agree on what goes where. This is why the next step isn't operational — it's conversational.

Your liaisons need to conduct a shared threat model conversation. Not merging your group's threat model with theirs — mapping the overlap. This is a different exercise than the individual and group threat models from the journal. You're not asking, "What are my risks?" or "What are our group's risks?" You're asking: "What risks does our coordination create?"

The questions that matter:

Where do our groups' activities create shared exposure? If both groups have been showing up to the same school board meetings, are you creating a pattern that connects the two groups publicly? If you coordinate a mutual aid delivery together, does the coordination itself reveal information about either group's membership or capacity?

What information about our coordination, if exposed, would create risk? The fact that two groups are talking to each other might be unremarkable — or it might not, depending on your context. The content of your coordination — who's doing what, when, where — is almost always more sensitive than the existence of the relationship itself. But both matter.

What stays internal to each group? Membership details. Internal disagreements. Individual members' personal situations. Your group's specific security vulnerabilities. These are not the other group's business, not because you distrust them, but because the principle holds: information that doesn't need to flow between groups shouldn't flow between groups.

This conversation will feel awkward. You're sitting down with people you're building trust with and talking explicitly about what you won't tell

each other. That awkwardness is a feature. Groups that don't have this conversation end up sharing everything by default — the merge instinct again — or sharing nothing and coordinating inefficiently because no one knows what's safe to communicate.

Inter-Group Information-Sharing Agreement

After the shared threat model conversation, write it down. Both groups keep a copy. This is an information-sharing agreement, and it doesn't need to be formal or legalistic — it needs to be clear. Here's a template:

Information that flows between groups (through the liaison channel): - Joint action logistics — meeting times, locations, division of responsibilities - Shared community intelligence — public meetings, events, local developments that affect both groups - Coordination requests — "We need help with X" or "We're planning Y, would your group be interested?" - Public-facing information about joint activities — what gets shared with the broader community

Information that stays internal to each group: - Membership details — who's in each group, how to contact them individually - Internal group dynamics — disagreements, interpersonal conflicts, decision-making processes - Individual members' personal information — addresses, workplaces, family details, personal situations - Group-specific security details — your specific threat model, your security vulnerabilities, your breach protocol details

Information that requires explicit consent before sharing: - Contact information for any individual member (requires that member's consent) - Details of any security incident (requires affected group's consent) - Anything involving a specific person's identity, circumstances, or situation (requires that person's consent)

The consent category is the one people forget, and it matters the most. In the course of coordination, one liaison might learn something about a member of the other group — someone's having a hard time, someone was at a specific event, someone has a particular skill that would be useful. The default should be: don't pass along information about specific people without their permission. This isn't bureaucracy. It's the security-as-care principle applied to the space between groups, where individuals are most vulnerable to having their information travel further than they intended.

Review the agreement together after your first joint action — you'll learn things about information flow that you couldn't have anticipated in advance. Adjust it. The agreement is a living document, not a contract.

There's one more scenario these notes need to address honestly, and it's the one nobody wants to talk about: what happens when something goes wrong with the other group.

I want to frame this carefully, because the wrong framing breeds the paranoia that destroys networks faster than any external threat.

Most security incidents between groups aren't infiltration. They're mundane. Someone from the other group mentions your joint activity in a context that wasn't agreed upon — at work, on social media, to a friend who wasn't supposed to know. Or someone leaves a group on bad terms and takes information with them — information that now crosses the boundary between groups because the departing member knew about the coordination. Or a group's security practices slip — disappearing messages get turned off, a member starts using an unsecured channel for sensitive discussions — and the liaison notices.

These aren't betrayals. They're the ordinary friction of human coordination, and the protocol handles them.

The Denver movement during the summer of 2020 shows what happens when these ordinary frictions meet the absence of any protocol at all.

Mickey Windecker was a paid FBI informant — a violent felon recruited to infiltrate the racial justice movement in Denver after the police killing of George Floyd. He arrived driving a silver hearse, presenting himself as a radical activist who'd fought with Kurdish forces overseas. Within weeks, he'd maneuvered into a position of influence across multiple activist groups. He recorded conversations. He pushed protesters toward increasingly aggressive actions, including discussions of assassinating the state's attorney general. He employed snitch-jacketing — accusing legitimate movement leaders of being informants to undermine their credibility and sow distrust.

Windecker succeeded not because he was sophisticated — his cover story was outlandish enough that some activists suspected him early on. He succeeded because the Denver movement had no boundaries between groups. No liaison structure. No information-sharing agreements. No protocol for assessing new people's trustworthiness over time. He moved freely across organizational lines because no organizational lines existed.

When activists began suspecting him, the accusations circulated chaotically — some people heard warnings, some didn't, some thought the warnings themselves were snitch-jacketing. The absence of structure meant that suspicion couldn't be investigated through any legitimate channel.

The result: multiple arrests, including one activist convicted on weapons charges after Windecker pressured him into buying a gun. Activists reported lasting trauma and a pervasive climate of distrust that fractured relationships for years. One activist described Windecker as having "started poking holes through everything" just as relationships and bonds were beginning to strengthen.

The lesson is not about informants. Most groups will never encounter an informant. The lesson is about what happens when coordination has no structure — when there are no boundaries between groups, no agreed-upon channels, no protocol for raising and investigating concerns. The same structural absence that let Windecker move freely would also let mundane security problems — a careless social media post, a bitter departure, a sloppy communication practice — cascade across the entire network.

The protocol for raising concerns between groups is direct and grounded in the same blameless approach from the journal's breach response:

If your liaison notices a security concern with the other group — a practice that seems careless, information appearing in unexpected contexts, a pattern that doesn't feel right — the conversation happens liaison to liaison. Not as an accusation. As a question: "We noticed X. Can we talk about how our groups handle Y?"

If the concern is about a specific incident — information was shared that shouldn't have been, a member's identity was exposed, coordination details appeared in a public context — the blameless breach protocol applies. What happened? What information was exposed? What's the realistic risk? What do we adjust? The goal is to fix the problem and update the agreement, not to assign fault.

If the concern is persistent and unresolved — the other group's security practices are genuinely inadequate and they're unwilling to address it — you have the option of limiting what flows through the liaison channel. Reduce the categories of shared information. Slow the cadence. You don't have to sever the relationship to protect your group. You can narrow the channel.

And if the concern is serious enough — if you genuinely believe the other group has been compromised or that coordination with them puts

your members at risk — you close the liaison channel. This is a last resort, and it should be a group decision, not an individual one. But the compartmentalization you've built means that closing one channel doesn't destroy everything else. Your group's internal security is intact. Your practices continue. The damage is contained, because you designed the structure to contain it.

This is what the Nebuchadnezzar's capture looks like in practice. Not a catastrophic network failure. A contained disruption that the rest of the network survives.

I want to close with something about the emotional weight of this chapter, because I've just asked you to sit with some uncomfortable ideas. Compartmentalization can feel cold — like you're building walls instead of bridges. The compromised-group protocol can feel paranoid — like you're planning for betrayal instead of building trust.

But think about what you're actually doing. You're building a structure that lets two groups coordinate safely, sustainably, and with clear expectations. The information-sharing agreement isn't a wall — it's a door with agreed-upon rules for when it opens and closes. The liaison model isn't a bottleneck — it's a bridge designed to carry the weight of real coordination. The compromised-group protocol isn't a plan for betrayal — it's a plan for the ordinary, human reality that things sometimes go wrong, and that having a plan for when they do is what lets you trust the structure.

Security as care. You've practiced it inside your group. Now you're extending it to the space between groups — the space where networks are built or broken.

Challenge

Establish a secure inter-group communication architecture with the other group:

1. Each group designates a liaison. Discuss the role with your full group first — the characteristics that matter, the boundaries of what the liaison can and can't commit to, the rotation cadence you'll use. Choose someone reliable, available, and disciplined about representing the group's decisions rather than freelancing.
2. Your liaisons create a shared Signal channel. Just the two liaisons — not

a merged group chat. Configuration: disappearing messages on (set a timer that works for both groups — 24 hours or one week are common starting points), notification previews off, Safety Numbers verified in person at your next boundary-spanner meeting.

3. The liaisons conduct a shared threat model conversation using the questions in this chapter. Where does your coordination create shared exposure? What information about your coordination would create risk if exposed? What stays internal?
4. Together, write an inter-group information-sharing agreement using the template above as a starting point. Adapt it to your context — the categories should reflect what your groups actually share and what actually needs to stay internal. Both groups keep a copy.

Document the agreement in your field journal. This is your first piece of network-level documentation — a shared protocol that both groups have created together. It won't be the last.

The first thing your liaison is likely to share through that new channel — once the architecture is in place and both groups have agreed on what flows — is something practical. A community event both groups should know about. A local development that affects you both. Maybe a question from their group about something your group has experience with.

Pay attention to the shape of that first exchange, because it will tell you something about what coordinating with this group actually feels like in practice. And pay attention to what comes up in the liaison channel that neither group could have anticipated — the shared concern that's bigger than either group expected, or the complementary capability that suggests you could accomplish something together that neither group can do alone.

That conversation — what could we do together? — is what the next chapter is about. But you're not ready for it until the channel is working, the agreement is signed, and both groups have experienced the reality of communicating across a structure that protects them both.

Build the architecture first. The coordination follows.

Summary

Inter-group coordination requires security architecture: a liaison model for structured communication, compartmentalization to limit information flow to what's nec-

essary, and a shared agreement about what flows between groups and what stays internal. The structure isn't about distrust — it's about ensuring that the trust you've built can survive pressure. When concerns arise, the protocol is blameless and direct. When the structure works, it turns security from a personal judgment call into a shared practice.

Action Items

- Designate a liaison in each group (reliable, available, disciplined about mandate)
- Create a shared Signal channel for the two liaisons with appropriate security configuration
- Conduct a shared threat model conversation mapping coordination risks
- Write and sign an inter-group information-sharing agreement
- Review the agreement after your first joint action and adjust

Case Studies & Citations

- **Underground Railroad compartmentalization.** Each conductor knew only their segment of the route. Structural information limits protected the network when individual nodes were compromised.
- **Alcoholics Anonymous autonomy tradition.** Each group autonomous except in matters affecting other groups or AA as a whole. Internal matters stay internal by structural design.
- **Zapatista nested governance.** Autonomous communities, municipalities, and regions make decisions at the level closest to those affected. Over thirty years of sustained resistance enabled by structural independence.
- **Indivisible statewide liaison model.** Designated representatives from local groups met regularly with clear mandates, enabling coordination among thousands of autonomous groups while containing disruptions.
- **Mickey Windecker / Denver FBI infiltration (2020).** Paid FBI informant infiltrated Denver's racial justice movement by exploiting the absence of inter-group boundaries, information-sharing agreements, and assessment protocols. Documented in FBI records and reporting by The Intercept. Resulted in arrests, distrust, and movement fragmentation.

Templates, Tools & Artifacts

- **Inter-Group Information-Sharing Agreement Template** — Three-category framework (flows between groups / stays internal / requires consent) with specific examples for each category (embedded above)
- **Liaison Role Description** — Characteristics, mandate boundaries, rotation cadence, and discipline guidelines
- **Compromised-Group Response Protocol** — Escalating response from liaison conversation through channel narrowing to channel closure

Key Terms

- **Compartmentalization** — The structural practice of limiting information flow between groups to what's necessary for coordination, protecting both groups from the consequences of any single point of failure
- **Liaison model** — A designated communication bridge between groups: one person per group carrying information according to shared agreements, rotating regularly to prevent bottlenecks
- **Information-sharing agreement** — A written document specifying what categories of information flow between groups, what stays internal, and what requires

explicit consent before sharing

- **Snitch-jacketing** — The practice of falsely accusing legitimate members or leaders of being informants, used to sow distrust and undermine movements from within. Also referred to as "bad-jacketing."

Chapter 29

Do Something Small Together

Your liaison channel has been open for a while now. Maybe a week, maybe a month — the timeline depends on your groups' pace and proximity. And something has already come through it. A community event both groups noticed independently. A school board agenda item that affects you both. A question from their group about something yours has experience with, or vice versa.

Pay attention to the shape of those early exchanges, because they contain the answer to the question this chapter is about: what could we do together?

Not what should we do, or what's the most important thing, or what would make the biggest difference. What *could* we do — practically, soon, with the resources and relationships we already have?

The answer should be something small. I want to explain why.

Your group completed a collective action during its work in Level 2. You know what it takes to plan something, execute it, and debrief honestly afterward. The other group has its own experience. Between you, there's plenty of capability.

The temptation is to match that capability to the scale of the problems you see. The school board is making decisions that affect both your neighborhoods — shouldn't you organize a coordinated response? There's a housing development threatening a shared community resource — shouldn't you build a real campaign?

Maybe. Eventually. But not yet.

The research on inter-group coordination is consistent on this point, and it's worth hearing clearly because it runs against every instinct: trust between groups is built through doing things together, not through agreements about doing things together. Ranjay Gulati's research on alliance formation found that repeated collaboration builds familiarity that func-

tions as trust — and crucially, that this familiarity reduces the need for formal governance structures later. Val Krebs and June Holley, studying network formation in Appalachian communities, put the practical implication plainly: early collaborative projects should be "initially small, so they can learn to collaborate."

Small doesn't mean unimportant. It means scoped so that the coordination itself is the learning. When two autonomous groups try to do something together for the first time, every step surfaces questions you can't anticipate in the abstract: How do we make a shared decision when our groups use different processes? Who speaks for the effort when we're talking to someone outside both groups? How do we divide work when we don't yet know each other's strengths in action? What happens when the plan needs to change and we can't all be in the same room?

These questions don't have theoretical answers. They have practical ones, and you find them by doing something small enough that the stakes are in the learning, not the outcome.

The Cowboy Indian Alliance understood this — though they might not have described it in those terms.

When Great Plains ranchers and Native American tribal communities first began working together to oppose the Keystone XL pipeline, they didn't start with a march on Washington. They started by showing up to the same places.

In November 2013, members of the Ponca Nation, the Ihanktonwan Dakota, and Nebraska ranchers gathered for a Spirit Camp on Art Tanderup's farm near Neligh, Nebraska — land that sat on both the proposed pipeline route and the historic Ponca Trail of Tears. Faith Spotted Eagle, an Ihanktonwan Dakota / Nakota elder, and Jane Kleeb of Bold Nebraska were among those who came together to bless the land, raise a tipi, and begin building relationships across communities that carried a hundred and fifty years of painful history in that part of the country. The gathering was small, ceremonial, grounded in place. Nobody signed a coalition agreement.

Those early relationships made everything that followed possible. When the Cowboy Indian Alliance organized the "Reject and Protect" campaign in April 2014 — tipis on the National Mall, thousands marching past the Capitol, national media attention — it grew from trust that had been built in a field, face to face, doing work that mattered in each community's own terms.

And the relationship kept deepening. In May 2014, members of the Ponca Nation returned to the Tanderup farm to plant Sacred Ponca Corn — the first time the tribe's ancestral seeds had been planted on their Nebraska homeland in over a hundred and thirty years. The action was ceremonial, grounded in place, and small in every measurable way. It didn't stop a pipeline. But it gave people something to do with their hands, side by side, on land that mattered to both of them. The annual plantings of Sacred Ponca Corn continued on the Tanderup farm for at least eight years — long after Obama rejected the Keystone XL permit in 2015, long after the political urgency had shifted. The practice that started as relationship-building became something more durable: a connection sustained by a shared act, not by a shared enemy.

That's what "small" means in this context. Not trivial. Foundational.

Now contrast that with what happens when groups have massive shared energy but no mechanism for doing things together.

Occupy Wall Street, at its peak in October 2011, had spread to over nine hundred cities. Hundreds of thousands of people shared a common analysis — the 99% versus the 1% — and a common physical presence. The energy was extraordinary. And the movement could not convert that energy into coordinated action, because it had built no structure for groups to plan, execute, and learn together.

You've already encountered OWS's internal structural problems — the consensus paralysis, the general assemblies that consumed hours without producing decisions. The inter-group problem was different and in some ways worse. When Occupy groups in different cities wanted to coordinate — a shared day of action, a response to a policy proposal, a mutual aid exchange — there was no mechanism. No liaison structure. No shared planning process. No way to make a decision that applied across groups without running it through each group's own consensus process, which could be blocked by any individual.

The result was that coordination happened informally — whoever had the most energy, the most social connections, or the most time ended up making decisions that affected everyone. Jo Freeman's diagnosis applied at every level: the absence of formal structure didn't eliminate coordination. It made coordination invisible, unaccountable, and fragile.

Political scientist John Ehrenberg captured the core failure in his analysis of OWS: process became the same as content. The movement treated the

act of deliberating together as equivalent to the act of doing something together. But deliberation without joint action doesn't build the inter-group trust that Gulati's research identifies. Only doing things together does that.

OWS changed American political discourse permanently. The 99% frame endured for a decade. But when the police cleared Zuccotti Park on November 15, 2011, the movement — with no organizational infrastructure independent of the physical occupation, and no inter-group coordination capacity — could not reconstitute.

The lesson is specific: doing something small together, with clear roles, a shared plan, and an honest debrief, builds more coordination capacity than any amount of shared analysis or values alignment. Agreement is not action. And trust is built in the doing.

So here's a planning tool. The Midwest Academy — a training institute for community organizers operating since 1973 — developed a strategy chart that forces specificity. Organizers have used it for campaigns. You're going to use it for one joint action.

The chart has five questions:

What's your goal? For a first joint action, the goal should be specific and achievable. Not "improve our neighborhood" — that's a direction, not a goal. "Attend the next city council meeting on the proposed zoning change with members from both groups present and prepared to speak during public comment" is a goal. "Host a skill exchange where each group teaches something the other group needs" is a goal. "Conduct a mutual aid delivery that covers a geographic area neither group reaches alone" is a goal. The specificity is the point — it forces you to agree on something concrete before you start coordinating.

Who has the power to give you what you want? For a first joint action, this might be straightforward — the city council, the school board, the community center director who controls the meeting space. Or it might not apply at all, if your action is internally focused like a skill exchange. But asking the question builds the habit of thinking about targets and decision-makers, which matters for everything that follows.

What organizational resources do you bring? Between two groups, you have people, skills, relationships, knowledge of your community, and whatever physical resources you've accumulated. Map them. The overlap is your foundation. The gaps between groups — where one has strength the other lacks — are where the collaboration adds value. If both groups bring

the same things, the joint action is just a bigger version of what each group could do alone. The point is complementarity.

Who are your allies and opponents? For a small first action, this might be a short list. But the exercise of thinking about it together — across groups, with different community knowledge — often surfaces information neither group had alone. Their group knows the council member who's sympathetic. Your group knows the neighborhood association that's been pushing back. The joint picture is richer than either group's individual view.

What tactics will you use? Tactics are the specific activities you'll undertake. Show up. Speak. Deliver food. Teach a skill. Host a listening session. The tactic should match the goal, fit your resources, and be something both groups can execute together. For a first joint action, simpler is better. The coordination is complex enough without adding tactical complexity on top of it.

Work through the chart together — both groups' liaisons, or if both groups agree, a small planning team of two or three people from each group. The conversation itself is valuable. You're making a shared decision for the first time, using a structured tool, and the process will reveal things about how your groups work together that no amount of conversation alone would surface.

Then do the thing.

The logistics matter more than they seem to. Who handles what? Who confirms the meeting space, or the supplies, or the transportation? Who communicates with any external parties — the council clerk, the community center, the families receiving mutual aid? Divide the responsibilities explicitly, based on each group's strengths. Don't default to whoever volunteers first — that's how informal hierarchy forms between groups, the same way it forms inside them.

Execute the plan. It doesn't need to go perfectly. First joint actions rarely do. Someone will miscommunicate a detail. A timing conflict will require last-minute adjustment. One group will feel like it did more of the work. These are not failures. They're data — and they're only useful if you capture them honestly.

Which brings us to the part that matters most.

The debrief.

Your group already knows how to debrief — you've been doing it since

your Level 2 work. The joint debrief uses the same foundation, adapted for the inter-group context. Run it within forty-eight hours of the action, while the experience is still fresh. Both groups together. A facilitator from one group — not the same group whose member facilitated the action, if possible. Notes taken and shared with both groups afterward.

Joint Debrief Protocol

The questions build on what you know:

What did we try to do? Start with a shared account of the plan. This sounds obvious but it matters — you'll sometimes discover that the two groups had subtly different understandings of the goal, even after planning together. Naming that gap early prevents it from distorting the rest of the debrief.

What worked? Be specific. Not "it went well" — what specifically went well? The coordination on logistics? The division of roles? The way one group's community knowledge complemented the other's? Specificity is what makes the success repeatable.

What was hard? This is where the debrief earns its value. The question isn't what went wrong — it's what was difficult. Communication gaps. Timing mismatches. Moments where one group's process conflicted with the other's. Places where autonomy and interdependence pulled in different directions — where one group wanted to make a decision and the other group hadn't been consulted. Name the friction honestly. You are not evaluating each other. You're evaluating the coordination, which belongs to both groups.

What would we do differently? Concrete adjustments, not abstract commitments. "We'd confirm logistics through the liaison channel 48 hours before, not 24" is useful. "We'd communicate better" is not.

What did we learn about working together? This is the question that only applies across groups, and it's the most important one. Not what you learned about the issue, the community, or the action's impact — what you learned about coordinating across the boundary between two autonomous groups. Where was the coordination smooth? Where did it chafe? Do your groups' decision-making styles complement each other or create friction? Would you want to do something together again — and if so, what would need to be different?

Write the debrief findings in your field journal. Both groups keep a copy.

This document is the foundation for everything in Phase 2 — it's your first shared record of what coordination between your groups actually looks like in practice, as opposed to what you hoped or planned it would look like.

In Orson Scott Card's *Ender's Game*, the early Battle Room exercises weren't designed for Ender's team to win. They were designed to teach a group of individuals how to coordinate under pressure — to move together, cover each other, adapt when the plan broke down. Ender understood something his commanders didn't always grasp: the victory was secondary. What mattered was whether the team learned to function as a unit. And the place where that learning actually happened wasn't the battle. It was the conversation afterward — what worked, what didn't, what to try next time.

The analogy isn't perfect. You're not in a battle, and your joint action isn't a test imposed by someone above you. But the structural insight is sound: the action is the exercise. The debrief is the curriculum. What you learn about coordinating together — through the friction, the adjustments, the honest assessment of what worked and what didn't — is worth more than the action's outcome. The outcome is temporary. The coordination capacity is what you keep.

Challenge

Plan, execute, and debrief one joint action with the other group:

1. Using the strategy chart framework above, plan a joint action small enough to succeed. Adapt to your context — the options include co-attending a public meeting with coordinated presence, hosting a joint skill exchange, conducting a mutual aid delivery that draws on both groups' networks, or organizing a community listening session in a neighborhood where both groups have connections. Choose something that requires genuine coordination between your groups, not just parallel attendance.
2. Divide responsibilities explicitly. Assign logistics, facilitation, external communication, and any other roles based on each group's demonstrated strengths. Document the division so both groups share the same understanding.

3. Execute the action.
4. Run a joint debrief within 48 hours using the protocol above. Both groups together. Honest about friction. Notes shared afterward.
5. Write the debrief findings in your field journal. What did you learn about working together? What would you change? What did the action reveal about your community or your shared interests that neither group knew before?

After the debrief, you'll have something you didn't have before: a shared experience with a documented assessment. You'll know whether your groups can coordinate, where the friction points are, and — just as important — what the coordination revealed about the terrain you share.

Pay attention to what surfaces in that debrief and in the liaison conversations that follow. The shared concern that turned out to be bigger than either group expected. The community connection made during the action that opens a door neither group could have opened alone. The moment when someone said, "We'd need more than just our two groups to actually address this."

That realization — that some things require more than two groups, that some questions don't have answers without governance structures, that some problems connect to institutions neither group has engaged with directly — is where Phase 2 begins. You'll recognize it when it arrives, because you'll have earned the vocabulary to name it. The coordination capacity you just built is the foundation for everything that follows.

But first: do the small thing. Learn from it. Write it down.

The debrief is the curriculum. The field journal is the record. And the record is how the network remembers what it learned.

`Summary`

Trust between groups is built through doing things together, not through agreements about doing things together. A first joint action should be small — scoped so the coordination itself is the learning. The Midwest Academy Strategy Chart provides a planning framework. The joint debrief is the most important part: it converts the experience into shared knowledge about how your groups actually coordinate, as opposed to how you hoped they would.

Action Items

- Plan a joint action using the Midwest Academy Strategy Chart (goal, power, resources, allies/opponents, tactics)
- Divide responsibilities explicitly between both groups
- Execute the action
- Run a joint debrief within 48 hours using the protocol above
- Record debrief findings in your field journal — both the structured responses and your group's internal reflections

Case Studies & Citations

- **Ranjay Gulati.** "Does Familiarity Breed Trust? The Implications of Repeated Ties for Contractual Choice in Alliances." *Academy of Management Journal* 38(1), 1995, 85–112. Foundational research showing that repeated collaboration builds familiarity functioning as trust, reducing the need for formal governance.
- **Val Krebs and June Holley.** Network formation research in Appalachian communities. Principle that early collaborative projects should be "initially small, so they can learn to collaborate."
- **Cowboy Indian Alliance (2013–2022+).** Nebraska ranchers, Ponca Nation members, and Ihanktonwan Dakota elders built relationships through a Spirit Camp (November 2013) on Art Tanderup's farm near Neligh, Nebraska — land on both the proposed Keystone XL pipeline route and the historic Ponca Trail of Tears. Those relationships enabled the "Reject and Protect" campaign (April 2014, National Mall, thousands marching) and the ongoing Sacred Ponca Corn plantings (first planted May 2014, continued annually for at least eight years). Faith Spotted Eagle (Ihanktonwan Dakota/Nakota elder) and Jane Kleeb (Bold Nebraska) were central to the coalition.
- **Occupy Wall Street (2011).** Spread to over 900 cities but could not convert shared energy into coordinated inter-group action due to absence of planning structures and liaison mechanisms. Cleared from Zuccotti Park November 15, 2011. John Ehrenberg's analysis: process became the same as content.
- **Midwest Academy.** Community organizer training institute, operating since 1973. Developed the strategy chart framework for campaign planning, adapted here for joint action planning.

Templates, Tools & Artifacts

- **Midwest Academy Strategy Chart (adapted)** — Five-question planning framework for joint actions: goal, power, resources, allies/opponents, tactics (embedded above)
- **Joint Debrief Protocol** — Five-question framework adapted for inter-group context: what we tried, what worked, what was hard, what we'd change, what we learned about working together (embedded above)

Key Terms

- **Joint action** — A coordinated activity planned and executed by two or more autonomous groups, with explicit division of responsibilities and a shared debrief
- **Complementarity** — The value that collaboration adds when groups bring different strengths, as opposed to simply scaling up identical capabilities
- **Strategy chart** — A planning tool that forces specificity about goals, targets, resources, allies, and tactics before action begins

Chapter 30

Decisions Without a Boss

Your joint debrief surfaced it. Maybe not in those words, but the question was there — in the moment someone asked "So do we just… keep doing things together?" and nobody had an answer for how that works. Or in the friction point about who decided the action's scope without checking with the other group first. Or in the honest admission that one group felt like it was following the other's lead and wasn't sure how that happened.

The question underneath all of it: who decides?

Inside your group, you have an answer. You built a consensus spectrum, ground rules, a rotating facilitator. You know how decisions work among five people who trust each other. Between groups, you have none of that — yet. And the stakes here are unambiguous, because the documented record is clear: the wrong answer to "who decides?" has destroyed more coalitions than any external threat. Not infiltration. Not opposition. Not lack of resources. Governance.

This chapter is the dense. It delivers three tools — a decision-making model, a framework for sorting which decisions belong where, and a template for a coalition agreement. They're practical. They're designed to be pulled off the shelf and brought to a meeting.

Consent Is Not Consensus

Your group uses a consensus spectrum — agree, reservations, stand aside, block. It works for five people who've built trust and share ground rules. It works less well the moment you add a second group, and it fails catastrophically at the scale of a coalition.

Consensus asks: does everyone actively agree? At Occupy Wall Street, that meant any single person in a general assembly of hundreds could block any proposal for any reason. The assemblies consumed months. Pro-

posals were modified until they were meaningless. Process devoured action — political scientist John Ehrenberg's postmortem in *Palgrave Communications* concluded that OWS treated deliberation as equivalent to doing something, and the movement paid for that confusion with its life. Zuccotti Park was cleared on November 15, 2011, and with no organizational structure independent of the physical occupation, OWS could not reconstitute.

You saw this dynamic in miniature inside your own group — the groan zone, the difficulty of moving from divergence to resolution. Now multiply that across groups that don't share ground rules, don't have the same facilitator, and may not even use the same decision-making vocabulary. Consensus across groups isn't slow. It's paralysis.

Consent asks a different question: does anyone have a reasoned, paramount objection?

The distinction was formalized by Gerard Endenburg in the Netherlands in the 1970s, building on cybernetics and Quaker governance traditions, and refined into what's now called sociocratic practice. John Buck and Sharon Villines documented the framework in *We the People: Consenting to a Deeper Democracy* — the most practical guide to consent governance for non-specialists. The core insight is that consent doesn't require agreement. It requires the absence of argued objections based on the group's shared purpose. "I'd prefer something different" is not an objection. "I'm not sure about this" is not an objection. "This would cause my group concrete harm, and here's why" is an objection.

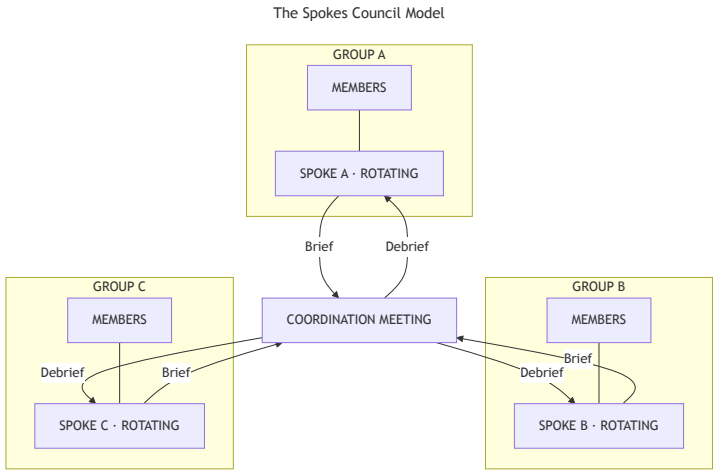
The threshold matters. Consent preserves every voice — anyone can raise a concern, and every concern gets heard. But it prevents any single voice from freezing the system. A paramount objection means the proposal is modified or tabled. Everything else moves forward. The result is governance that's slower than unilateral decision-making and faster than consensus. For coordinating autonomous groups, that's the operative range.

The pattern is consistent enough in the documented record to treat as a finding, not a preference: every durable multi-group coordination structure I found in the research uses some version of consent, whether or not they call it that. The International Association for Facilitators' delegates assemblies. Mondragon's cooperative congress. The Quaker practice of "sense of the meeting." The spokes councils that emerged from the 1999 WTO protests. None of them require unanimity. All of them require that objections be reasoned and grounded in shared purpose.

The Spokes Council

The practical structure for consent-based governance between groups is a spokes council. The concept originated in anarcho-syndicalist organizing during the Spanish Civil War and was refined during the anti-globalization movement. Occupy Sandy improved the model by organizing around projects rather than identity groups — a pragmatic adaptation that made the structure functional for coordinating hundreds of volunteers and managing substantial resources through consent.

Here's how it works for your coordination:



Each group designates one rotating delegate — the spoke. The spoke attends joint coordination meetings, carries their group's input, and has a defined mandate: what they can agree to on behalf of their group during the meeting, and what requires bringing back for discussion. The mandate is specific, not general. "You can agree to meeting times and logistics" is a mandate. "Use your best judgment" is not — it's a blank check, and blank checks are how informal hierarchy forms between groups.

The spokes meet regularly — every two weeks is a reasonable starting cadence, adjusted to what your coordination actually requires. Decisions are made by consent among the spokes: a proposal is presented, concerns are heard, and if no spoke raises a paramount objection, the proposal moves forward. If an objection is raised, the proposal is modified to address it. If it can't be modified to everyone's satisfaction, it's tabled — which means the groups don't coordinate on that specific thing, not that

the coordination fails.

The rotation matters. The spoke role shifts — monthly or quarterly, whatever the groups agree — so that no one person becomes the permanent representative, and so that multiple group members develop the skill of inter-group coordination. This is the same principle as rotating facilitation inside your group, applied at network scale. The person who represents you this month isn't your leader. They're your current communication node.

Two practical details that seem minor and aren't. First: spokes should brief their group before each coordination meeting (what's on the agenda, what positions the group holds, what the spoke's mandate covers) and debrief afterward (what was decided, what's pending, what's coming next). The brief-and-debrief cycle is what keeps the spoke accountable to the group rather than becoming an autonomous actor. Second: when possible, groups should sit together during coordination meetings so the spoke can consult in real time — a quick "Can I agree to this on our behalf?" during a meeting is faster than tabling everything for consultation.

`Spokes Council Protocol`

Before the meeting: Each group's spoke confirms the agenda with their group, clarifies the mandate (what they can agree to, what requires group consultation), and gathers input on known agenda items.

Opening: Confirm who's present, review the agenda, note any time constraints. Rotating facilitation between groups — the facilitator should not be a spoke for this meeting if possible.

For each proposal: Present the proposal clearly. Round of reactions — each spoke shares their group's perspective. Identify concerns. Modify the proposal if needed. Test for consent: "Does any spoke have a paramount objection — a reasoned concern that this would cause your group harm?" If no objections, the proposal is adopted. If an objection is raised, address it — modify, table, or separate the issue from the broader coordination.

Closing: Review decisions made. Identify what each spoke needs to bring back to their group. Set the next meeting. Each spoke debriefs their group within 48 hours.

Decision Domains

The spokes council handles joint decisions. But not every decision is joint, and one of the fastest ways to create friction between autonomous groups is to treat internal decisions as if they require inter-group consent — or to treat joint decisions as if one group can make them alone.

Decision domains are the concept that different decisions belong at different levels. This sounds obvious. It isn't — or rather, it's obvious in principle and remarkably easy to get wrong in practice. The Democratic Socialists of America's 200-plus chapters discovered this the hard way.

DSA's federated model enabled extraordinary growth — over 100,000 members, anyone could start a chapter, and chapters became centers of political engagement that produced real electoral victories. But the model produced what internal analysts described as disconnected pools: no visibility between chapters, no two chapters' bylaws particularly similar, and chapters interacting on what one DSA publication described as "a very haphazard basis." The most visible fracture came in 2024, when NYC-DSA — the largest chapter, operating as a legally distinct entity that raises its own funds and runs its own campaigns — voted to reendorse Alexandria Ocasio-Cortez after the national leadership withdrew DSA's endorsement over a policy dispute.

The lesson isn't that DSA's federalism failed. It's that federalism without explicit decision domains — without a shared understanding of what belongs to chapters and what belongs to the whole — creates friction that becomes structural. Nobody defined the boundaries, so the boundaries were discovered through conflict. By the time the friction surfaced, the patterns were entrenched.

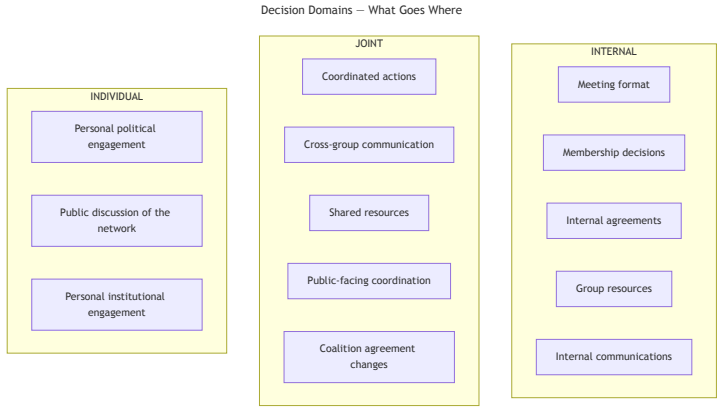
Contrast that with Mondragon.

The Mondragon Corporation is a federation of worker cooperatives in the Basque region of Spain — currently 81 cooperatives employing over 70,000 worker-members, generating roughly €11 billion in annual revenue, governed through nested democratic assemblies from individual cooperatives up through divisional groupings to a Congress of 650 delegates. The structure has sustained since its founding in 1956. It is the most successful large-scale democratic governance model in the documented record.

Mondragon works because decision domains are explicit at every level. Each cooperative governs itself — its internal operations, hiring, production decisions. The divisional groupings coordinate shared services — pur-

chasing, R&D, finance. The Congress sets broad strategic direction and manages the shared principles that hold the federation together. A decision about a single cooperative's work schedule doesn't go to the Congress. A decision about the federation's strategic investments doesn't get made by a single cooperative. Everyone knows what's decided where, which means the energy goes into the decision itself rather than into arguing about who has the authority to make it.

Your coordination doesn't need Mondragon's complexity. But it needs the same clarity. Here's a framework for mapping your decision domains:



`Decision Domain Mapping Template`

Internal to each group (decided by each group independently — the other group has no vote): - How you run your own meetings - Who you admit as members - Your group's internal agreements and ground rules - How you spend your own resources - Your group's internal communication practices - *(Add your own — what else is yours alone?)*

Joint decisions (decided together through the spokes council — neither group acts unilaterally): - What actions you coordinate on together - How you communicate across groups (liaison protocol, shared channels) - Shared resources — what you pool and how it's managed - Public-facing coordination — anything that represents both groups to the outside world - Changes to the coalition agreement - *(Add your own — what else requires both groups?)*

Individual decisions (belonging to each person — neither the group nor the coordination governs these): - Each member's personal political

engagement - How individuals talk about the network publicly, within the bounds of security agreements - Whether and how individuals engage with institutions in their personal capacity - *(Add your own — what else is personal?)*

Gray areas (not yet sorted — discuss and assign): - *(This is where the conversation gets productive. What decisions don't clearly fit? Name them, discuss them, assign them.)*

Work through this together at a joint meeting. The conversation is the point. You'll discover that most items sort easily — you'll know immediately that your group's meeting time is internal and that a joint public action is joint. The interesting moments are the gray areas: Is social media posting about the coordination a joint decision or individual? If one group wants to engage with a local institution, does the other group get a voice? These edge cases are where the real governance lives, and they're far better sorted in a calm conversation now than discovered during a conflict later.

When the Spokes Council Disagrees

The three tools above — consent, the spokes council, and decision domains — handle most coordination governance. But there's a harder version of the problem: what happens when the groups disagree not on a specific proposal but on direction?

Amanda Tattersall's research on coalition durability, documented in *Power in Coalition*, offers the clearest framework. Her three-step approach, adapted here for your context:

Step one: Clarify whether the disagreement is about goals or methods. Most disagreements between coordinating groups are about methods — how to do something, not whether to do it. One group wants to attend the city council meeting. The other wants to organize a community forum first. Both groups want civic engagement. They disagree on the approach. When the shared goal is restated clearly, method disagreements often dissolve — or become a productive "both/and" rather than "either/or." One group attends the council meeting while the other organizes the forum. The coordination supports both.

Step two: If the disagreement is about goals, surface whether the interests are genuinely incompatible or just differently prioritized. Your

groups came together because of overlapping concerns — but your priorities may not be identical. One group is focused on housing. The other is focused on school board accountability. These aren't incompatible. They're different facets of the same civic engagement. A coalition doesn't require unanimous priorities. It requires enough shared ground to act on something together. Tattersall's research found that the strongest coalitions have "both common and separate interests" — pure overlap leads to competition for the same resources and recognition, while complementary interests create mutual need.

Step three: If interests are genuinely incompatible on a specific issue, agree to disagree — and keep coordinating on everything else. This is the step most coalitions skip, and it's why they fracture. The assumption is that a disagreement on one issue means the coordination has failed. It hasn't. It means the coordination has found a boundary. Your groups don't coordinate on that issue. You continue coordinating on everything you do share. The coalition agreement reflects this: the boundary is named, documented, and respected. No one pretends the disagreement doesn't exist. No one treats it as a betrayal.

The Women's March is the cautionary tale for what happens without this framework. A coalition of over 550 partner organizations, the largest single-day protest in U.S. history — undone not by opposition but by an internal accountability crisis that the coalition had no mechanism to resolve. No escalation protocol. No decision domains. No way for the broader coalition to force action when four co-chairs held concentrated, unaccountable authority. When co-chair Tamika Mallory's association with Louis Farrakhan and the ensuing antisemitism controversy surfaced, the coalition had no governance to process it. Co-founder Teresa Shook had to resort to a Facebook post to call for resignations. By the time three of the four co-chairs departed in September 2019, partner organizations had dropped from 550 to roughly 200. State chapters had dissolved. The coalition that mobilized millions of people couldn't sustain itself through one unresolved internal conflict.

The lesson isn't that the underlying disagreement was too hard. It's that no structure existed to process it. You have the tools to do better. Use them before you need them.

In David Fincher's *Fight Club*, the rules were the governance. "The first rule of Fight Club" wasn't about secrecy — it was about establishing a

shared framework that every member understood. The rules created something remarkable: a distributed, leaderless structure where anyone could start a new chapter and the rules held the thing together without a central authority.

Then Tyler Durden started Project Mayhem. The rules changed. Suddenly decisions were made unilaterally — by one person, for everyone, without consent. Members were told not to ask questions. The distributed governance collapsed into hidden hierarchy, and by the time anyone noticed, the structure had become the opposite of what the rules promised.

The film is a cautionary tale about the gap between stated governance and actual governance. Fight Club's rules said "distributed." Tyler's behavior said "centralized." The people following the rules didn't notice the shift because the rules were still technically in place — they just weren't the actual decision-making structure anymore. Jo Freeman diagnosed this pattern decades before the film: in "The Tyranny of Structurelessness," first published in *The Second Wave* in 1972, she argued that eliminating formal hierarchy doesn't eliminate hierarchy. It makes hierarchy invisible, unaccountable, and harder to challenge.

The spokes council, the decision domains, and the coalition agreement exist precisely to prevent that shift. Not because anyone in your coordination is Tyler Durden — but because the drift from distributed governance to informal centralization happens so gradually that you don't notice it until someone's making decisions for everyone and nobody agreed to that.

Name the structure. Write it down. And when someone acts outside it, the documentation makes the conversation possible.

Challenge

At a joint meeting of both groups — all members, not just liaisons — establish your coordination governance:

1. **Adopt consent-based decision-making through a spokes council.** Each group designates its first spoke. Define the spoke's mandate explicitly: what can they agree to in a coordination meeting, and what requires bringing back to the group? Set a rotation schedule. Agree on a meeting cadence for the spokes council — start with every two weeks and adjust.
2. **Map your decision domains together.** Using the template above, sort

decisions into internal, joint, individual, and gray areas. Spend real time on the gray areas — they're where the governance earns its value. Both groups keep a copy of the completed map.

3. **Practice a real consent decision.** Pick something concrete — the next joint action, a shared resource allocation, a communication protocol adjustment. Run the consent process through the spokes council. Present, react, modify, test for objections. The practice matters more than the outcome. If the consent process feels clunky the first time, that's expected. The second time is faster.
4. **Write a coalition agreement.** Not a constitution — a one-page document that states:

`Coalition Agreement Template`

Who's in this coordination: *(Name the groups. Identify their current spokes.)*

How decisions are made: *(Consent-based, through the spokes council. Define the objection threshold. Note the rotation schedule.)*

What's shared and what's autonomous: *(Attach or reference the decision domain map.)*

How disagreements are handled: *(The three-step escalation: goals vs. methods → compatible vs. incompatible interests → agree to disagree and continue coordinating on shared ground.)*

How this agreement changes: *(Changes to the agreement itself are joint decisions requiring consent from all groups. Review the agreement at an agreed interval — quarterly is reasonable.)*

Signed by: *(Spokes on behalf of their groups, with the understanding that each group ratified the agreement through their own decision-making process.)*

This is the entry fee for sustained coordination. It's not the exciting part. It's not the joint action or the community impact or the growing network. It's the structural foundation that makes those things possible without one group dominating, without decisions happening in hallways instead of meetings, without the slow drift toward informal hierarchy that has killed movements with far more resources and energy than yours.

You've paid entry fees before. Inside your group — the ground rules, the consensus spectrum, the facilitator role, the agreements that felt bureaucratic until the first conflict proved they were essential. This is the same thing, at a different scale. The groan zone between groups feels different

from the groan zone inside one. It's less personal and more structural. The friction is about pace and priority and process, not about whether people like each other. And the tools that resolve it are structural too — not deeper relationships (though those help), but clearer agreements about how the coordination works.

Write the coalition agreement. Practice the consent decision. Map the domains. And file all of it in your field journal, because the next time you need to reference what you agreed to — and you will — it should be findable.

Field journal: Record the completed decision domain map, the coalition agreement, and your group's internal notes on how the consent process felt. What was easier than expected? What was harder? Where did the gray areas in the decision domain mapping surprise you? And — this one matters for what comes next — what came up during the governance conversation that connects to the world outside your coordination? An institution one group mentioned. A local issue that both groups' decision domains touch. A realization that some of the decisions you're mapping don't just involve your two groups — they involve the civic landscape you're both part of. Note that. The next chapter is about that landscape.

Summary

Governance is the most common cause of coalition failure — more than opposition, infiltration, or lack of resources. This chapter introduces consent-based decision-making (where proposals move forward unless someone raises a reasoned, paramount objection), the spokes council (a rotating delegate structure for inter-group coordination), and decision domain mapping (sorting which decisions belong to individual groups, to the coalition, or to individual members). A coalition agreement documents these structures. When groups disagree, a three-step escalation — goals vs. methods, compatible vs. incompatible interests, agree to disagree — prevents fracture.

Action Items

- Designate first spokes and define their mandates
- Map decision domains at a joint meeting, with particular attention to gray areas
- Practice a real consent decision through the spokes council
- Write and sign a coalition agreement
- File all governance documents in the field journal

Case Studies & Citations

- **Occupy Wall Street / John Ehrenberg** — Ehrenberg, "What Can We Learn from Occupy's Failure?" *Palgrave Communications*, 2017. Political scientist at Long Island University. OWS general assemblies as cautionary case for consensus-at-scale. Zuccotti Park cleared November 15, 2011.
- **Gerard Endenburg / Sociocratic practice** — Endenburg developed the Sociocratic Circle-Organization Method in the 1970s at Endenburg Elektrotechniek, drawing on cybernetics and Quaker governance traditions. Buck and Villines, *We the People: Consenting to a Deeper Democracy*.
- **Mondragon Corporation** — Federation of 81 worker cooperatives, Basque Country, Spain. Over 70,000 worker-members, ~€11 billion annual revenue. Founded 1956. Congress of 650 delegates. Nested democratic assemblies with explicit decision domains at every level.
- **DSA federated model** — Democratic Socialists of America, 200+ chapters. Federated structure without explicit decision domains produced structural friction. NYC-DSA/national leadership AOC reendorsement dispute (2024) as illustrative case.
- **Women's March (2017–2019)** — Coalition of 550+ partner organizations. Sponsors dropped from 550 to ~200 by 2019. Internal accountability crisis with no governance mechanism to resolve it. Four co-chairs with concentrated authority; three departed September 2019.
- **Amanda Tattersall** — *Power in Coalition*. Coalition durability research. Three-step framework: goals vs. methods, compatible vs. incompatible interests, agree to disagree.
- **Jo Freeman** — "The Tyranny of Structurelessness," first published in *The Second Wave*, 1972. Also published in *Berkeley Journal of Sociology*, Vol. 17, 1972–73, pp. 151–165. Informal hierarchy in ostensibly structureless groups.
- **Occupy Sandy** — Spokes council organized around projects rather than identity groups. Adapted model for volunteer coordination and resource management.

Templates, Tools & Artifacts

- **Spokes Council Protocol** — Pre-meeting preparation, opening, proposal process, consent test, closing and debrief cycle
- **Decision Domain Mapping Template** — Four categories: internal, joint, individual, gray areas
- **Coalition Agreement Template** — One-page document covering membership, decision-making, shared/autonomous domains, disagreement handling, amendment process

Key Terms

- **Consent (governance)** — Decision-making method where proposals move forward unless a participant raises a reasoned, paramount objection. Distinct from consensus (which requires active agreement).
- **Paramount objection** — A reasoned concern that a proposal would cause concrete harm to a group's ability to fulfill its shared purpose. Preferences and uncertainties are not paramount objections.
- **Spokes council** — A coordination structure where each group sends a rotating delegate (spoke) with a defined mandate to make inter-group decisions by consent.
- **Decision domains** — The sorting of decisions into levels (internal, joint, individual) so that the right decisions are made by the right people at the right scale.

- **Coalition agreement** — A written document establishing how coordinating groups make decisions, what's shared and what's autonomous, and how disagreements are handled.

—

Chapter 31

The Landscape Around You

Something came up during your governance work. Maybe it was explicit — a specific institution that one group's spoke mentioned during the decision domain mapping, a local organization that both groups interact with but haven't approached together. Maybe it was subtler — a realization that some of the decisions you were sorting into "joint" don't just involve your two groups. They involve a school board, a county commission, a mutual aid network that's been operating in your area longer than either of your groups has existed. Your coordination doesn't happen in a vacuum. It happens on ground that's already occupied.

This chapter is about that ground. The institutional landscape — who's already working in your community and how your network engages without being absorbed. The legal landscape — what the law says about your rights and your exposure when you take coordinated civic action. And the geographic landscape — what all of this looks like when the nearest allied group is forty miles away or the civic infrastructure is a volunteer fire department and a church.

The throughline is the same: know the terrain you're operating on. All three are maps — and the purpose of a map is to move through a landscape more effectively, not to admire it from a distance.

The Institutional Landscape

Your network exists within a field of institutions. Neighborhood associations, faith communities, mutual aid networks, PTAs, local government bodies, nonprofits, unions, civic organizations. Some have been in your area for decades. Some formed last year. Some are well-funded and professionally staffed. Some run on volunteer energy and borrowed meeting space.

The question isn't whether to engage with them. Your groups are already engaged — as individuals, you attend meetings, donate time, participate in institutional life. The question is how your network relates to institutions as a network. And the honest answer is: carefully.

There's a dynamic that the research identified in virtually every documented case of grassroots-institutional interaction, and naming it is the only protection against it. The sociologist Philip Selznick studied the Tennessee Valley Authority in the 1940s and documented how a federal agency absorbed grassroots opposition by channeling it — offering local leaders seats on advisory boards, creating the appearance of influence without transferring actual decision-making power. The pattern he identified has three mechanisms, and they operate today the same way they did eighty years ago.

Channeling. The institution redirects grassroots energy into its own processes. You came to push for change. You end up on a committee that meets quarterly and advises a board that isn't required to act on your advice. Your energy is now serving the institution's legitimacy rather than your community's priorities. The institution can point to your participation as evidence of community engagement. You can point to nothing that's changed.

Inclusion without power. A seat at the table without a voice in decisions. You're invited to meetings, copied on emails, thanked for your input. But the decisions that matter — budgets, hiring, policy — happen in rooms you're not in, through processes you can't influence. The inclusion is real. The power is not.

Salience control. The institution appears to address your concerns by highlighting the overlap between your priorities and its existing work — while quietly excluding the areas where your priorities challenge its operations. You came to talk about housing displacement. The meeting agenda focuses on a new community garden program. Both are real needs. But the garden isn't why you're here, and the displacement isn't on the agenda.

These mechanisms aren't malicious. They're structural. Institutions operate by institutional logic — continuity, stability, process, self-preservation. That logic tends to domesticate informal energy. A PTA's job is to support the school, not to challenge the district. A nonprofit's funding depends on its funders' priorities, which may not be yours. A local government body's processes are designed to manage participation, not to empower it. None of this makes institutions adversaries. It makes them institutions. And

knowing how they work means your network can engage without being consumed.

The model the documented record supports is complementary partnership — a term from Amanda Tattersall's coalition research. Your network engages institutions as a partner, not a subordinate. You bring skills, flexibility, and the capacity for rapid coordinated action. They bring infrastructure, history, institutional knowledge, and public legitimacy. Neither absorbs the other. The relationship is defined by the specific thing you're working on together, not by a general alliance.

The Cowboy Indian Alliance operated this way. Ranchers and tribal communities maintained distinct identities, distinct motivations, and distinct organizational structures while coordinating on the Keystone XL fight. They didn't merge into one organization. They didn't adopt each other's frameworks. They agreed on one thing — opposing the pipeline — and maintained autonomy on everything else. When the fight shifted, each group remained intact, with its own relationships and its own capacity. The coalition didn't hollow them out.

Your network decides its own institutional posture through conversation — not through these notes and not through a blanket stance. Some institutions in your landscape will be natural partners. Some will be worth engaging cautiously. Some won't be worth your coordination's time. The institutional mapping challenge helps you sort that collectively.

The Legal Landscape

When your network starts taking joint action visible in civic space — attending government meetings as a coordinated presence, filing public records requests, organizing a community event — the legal environment becomes relevant terrain. This isn't preparation for confrontation. It's the civic equivalent of knowing where the fire exits are.

I'm not a lawyer, and these notes aren't legal advice. What I can do is point you to the resources that will give your network legal awareness — enough to know your rights, recognize when you need professional counsel, and avoid the most common mistakes that groups make when they don't understand the legal ground they're standing on.

Your right to assemble and petition. The First Amendment protects

your right to gather, protest, petition, and speak on matters of public concern. State and local laws layer additional regulations on top — permit requirements, restrictions on amplified sound, designated free-speech zones, anti-camping ordinances. These regulations vary enormously by jurisdiction, and they've shifted significantly in recent years. The International Center for Not-for-Profit Law maintains a US Protest Law Tracker that maps state-level legislation affecting protest rights — hundreds of bills introduced across all 50 states since 2017, with new restrictions on assembly, increased penalties for civil disobedience, and provisions affecting how protests near critical infrastructure are treated. Check it for your state. The landscape is specific to where you are.

Your right to observe government proceedings. City council, county commission, school board, planning board — these are public proceedings. You have the right to attend, observe, and in most cases record. Your right to speak during public comment periods is governed by local rules that vary but generally must be applied evenhandedly — a board can't allow one group to speak and deny another on the basis of viewpoint. Knowing these rules before you attend matters more than it should.

Your right to public records. The Freedom of Information Act applies to federal agencies. Every state has its own public records law with different scopes, exemptions, and response timelines. The National Freedom of Information Coalition maintains state-by-state guides, template request letters, and guidance on fee waivers. Filing a public records request on behalf of a community interest often strengthens fee waiver arguments, since the information serves the public rather than a private commercial purpose.

When you need a lawyer. If your network is considering any action that carries legal risk — civil disobedience, activities near critical infrastructure, engagement with law enforcement, anything involving permits or regulatory compliance — consult a lawyer first. The National Lawyers Guild maintains a chapter locator at nlg.org and runs legal observer trainings for community groups. Local legal aid organizations can help with public records, government meeting access, and understanding local ordinances. The ACLU's Know Your Rights guides — available in multiple languages — cover demonstrations, encounters with police, and the right to record. Distribute them to all network members. They're free, they're clear, and knowing the basics prevents most of the situations where not knowing them causes harm.

This isn't a comprehensive legal education. It's an orientation to the

terrain. Your field journal should include the specific resources for your state — the ICNL tracker results, the relevant ACLU guides, the nearest NLG chapter contact, and local legal aid organizations that serve your area. Like the institutional map, the legal map is specific to your geography.

The Geographic Landscape

Everything I've described so far assumes an institutional landscape that's reasonably populated. Organizations to map. Government meetings to attend. Multiple community groups operating in overlapping territory. In many parts of the country, that assumption holds.

In many other parts, it doesn't.

If your network is in a rural area, a small town, or an exurban community where the civic landscape is sparse, the challenge isn't navigating a crowded field. It's finding civic life where it's thin on the ground — and recognizing it in forms that urban-centric organizing frameworks don't always see.

I want to be direct about this because the research was clear: the organizing literature has a density bias. Most case studies, most frameworks, most practical guides assume you can walk to a meeting, that there are multiple organizations within driving distance, that broadband is reliable and the nearest allied group is across town rather than across a county. When rural communities appear in organizing literature at all, they tend to appear as problems — connectivity gaps, isolation, limited institutional infrastructure. That framing misses something important.

Rural America has deep organizing traditions that predate any urban equivalent. Cooperative federations — the Farm Bureau, the Grange, rural electric cooperatives — built durable coordination infrastructure across enormous distances before the telephone was common. The circuit rider model, where a single organizer or minister served multiple communities on a rotating schedule, created connection across sparse networks for two centuries. County-based mutual aid — neighbors helping neighbors with harvest, with illness, with fire — is the oldest form of collective action in the country. Sparse networks are often deeper. Fewer connections, but each one carries more weight.

The discovery protocols for finding civic life in low-density areas look

different from urban institutional mapping, but the principle is the same: look for where people already gather, already coordinate, already make decisions together.

County commissioner meetings — in rural areas, often the most accessible and impactful tier of government. They control land use, roads, emergency services, and local budgets. Meetings are public, frequently sparsely attended, and your presence is noticed. That's both an advantage and a consideration.

Faith communities — churches, mosques, synagogues — serve as the primary gathering infrastructure in many rural areas. They host meetings, coordinate mutual aid, maintain communication networks, and often function as the de facto civic space. Engaging with them doesn't require sharing their faith. It requires respecting their role and showing up as a community partner.

Volunteer fire departments — in communities without professional fire services, often the most trusted civic institution in the area. They run on the same principle your group does: ordinary people taking responsibility for their community's safety. Their fundraisers, community dinners, and workdays are gathering points where you meet the people who actually make the community function.

Libraries — in rural areas, often serving as community centers, meeting spaces, internet access points, and information hubs. Library bulletin boards and event calendars are low-tech discovery tools that tell you what's happening and who's organizing it.

Agricultural extension offices — the cooperative extension system has maintained a presence in nearly every county in the country for over a century. Extension agents work with farmers, 4-H programs, community development, and food security projects. They know the civic landscape of their county better than almost anyone.

These aren't second-best alternatives to an urban institutional field. They're the actual civic infrastructure of communities that have been self-governing for generations. Your institutional mapping adapts to this terrain — map what exists, understand who serves what function, and identify where your network's skills and energy complement what's already in place.

The distance question is real. When your nearest allied group is forty miles away, a joint meeting requires planning, travel time, and the logistical coordination that urban networks take for granted. Hybrid meetings — some members in person, some on a call — are a practical necessity, not a

compromise. The spokes council model from the last chapter works well for geographic distance: the spokes meet in person or hybrid, carry their groups' input, and debrief afterward. The coordination doesn't require everyone in the same room. It requires reliable communication channels and clear mandates.

Down Home North Carolina demonstrates what permanent rural infrastructure looks like at scale. Founded in 2017, Down Home built county-based chapters across 25 rural North Carolina counties — a footprint spanning roughly 500 miles. Each county chapter operates with local autonomy, elects its own leadership, and sets priorities based on local concerns. Paid local organizers stationed in each region provide continuity that volunteer-only models struggle to maintain. Statewide coordination happens through regular convenings where county chapters share strategy and align on shared campaigns without surrendering local control.

The results are documented. Across the 2020 and 2022 cycles, Down Home's canvassing operation reached over 600,000 doors across those 25 counties. In districts they organized, results consistently bucked the national rightward trend — not by converting voters but by engaging people who had stopped participating. Year-round organizing rather than campaign-season-only contact built relationships that survived between election cycles. The infrastructure persisted because it was rooted in place, maintained through cycles, and didn't depend on any single leader or external funder.

Compare that with the Georgia 2020 Election Protection Coalition. Ten organizations turned a state — Fair Fight handled litigation, New Georgia Project focused on registration, Black Voters Matter provided grassroots tools, Asian Americans Advancing Justice–Atlanta provided language access. Specialized division of labor and complementary capabilities produced extraordinary results: 800,000 new voters registered, a state flipped. But the model depended on a single charismatic leader's profile for fundraising, and the operational infrastructure was sustained by external money rather than local roots. By 2025, both Fair Fight and the New Georgia Project had closed. The voters they registered were still there. The infrastructure that engaged them was not.

The lesson isn't that institutional coordination fails. The Georgia coalition succeeded spectacularly at what it set out to do. The lesson is that institutional dependency — infrastructure that's borrowed rather than built,

capacity that evaporates when funding or leadership shifts — is fatal to long-term civic presence. Down Home's model persists because the infrastructure belongs to the counties it serves. Georgia's produced extraordinary results and left nothing permanent behind.

Your network's engagement with institutions — whether in a dense urban field or across rural counties — should aim for the former. Build relationships with institutions. Benefit from their resources and knowledge. But ensure that your network's capacity is yours, not borrowed.

In the Hulu adaptation of Margaret Atwood's *The Handmaid's Tale*, June Osborne doesn't have the luxury of working only with people she trusts. She works with Commander Lawrence — a man who helped design the system that enslaved her — because his resources, his guilt, and his remaining institutional access are useful. She coordinates with Marthas across class boundaries, building an operational network out of people whose positions within Gilead's hierarchy give them access her position denies. She engages the Mayday resistance without knowing its full structure or fully trusting its leadership.

June's coalition-building is pragmatic. She doesn't pretend Lawrence is a genuine ally. She doesn't confuse the Marthas' cooperation with ideological alignment. She works with imperfect partners because the mission — getting children out — requires capabilities no single person or group possesses. The moral complexity of that engagement is the point. You can work with institutions whose values don't perfectly align with yours, whose structures reproduce dynamics you're working to change, whose leadership may be part of the problem you're trying to address. The question isn't whether the partnership is pure. It's whether it serves the mission while preserving your network's autonomy.

That's the landscape question at its sharpest. Know the institutions. Know the law. Know the ground. And know what you're engaging for, what you're offering, and what you're not willing to trade.

Challenge

Three parts, adapted to your geographic context.

Part 1 — Map your institutional landscape. At a joint meeting, identify the organizations active in your area. For each one:

- **Name and function:** What does this organization do?
- **Constituency:** Who does it serve or represent?
- **Overlap:** Where do its interests intersect with your network's concerns?
- **Engagement history:** Has anyone in the network already interacted with it?
- **Opportunity:** What could a partnership look like?
- **Co-optation risk:** Where might the channeling, inclusion-without-power, or salience control dynamics apply?

For urban and suburban networks, prioritize — not every institution warrants network-level engagement. Focus on organizations whose work is complementary to your current concerns.

For rural networks, map what exists. A short list isn't a weak map — it's an accurate one, and it tells you exactly where your engagement has the most leverage.

Part 2 — Make one institutional contact as a network. Not as individual groups — as a coordinated network. Attend an institutional event together, or invite an institutional representative to a joint meeting, or propose a specific collaboration. The contact should be deliberate: the network has discussed what it wants from the relationship and what it's offering.

Be transparent about who you are — an informal network of community members working on local concerns. Don't overstate your capacity. Don't understate your commitment.

Part 3 — Build your legal awareness file. This can be done concurrently with the institutional mapping:

1. Check the ICNL US Protest Law Tracker for your state's specific legislation affecting assembly, protest, and civic action.
2. Download and distribute the ACLU Know Your Rights guides to all network members.
3. Identify your nearest NLG chapter and local legal aid organizations. Add their contact information to the network's shared resources.
4. At a joint meeting, conduct a 30-minute orientation: your right to attend and record public meetings, the basics of your state's public records law, and when to consult a lawyer.

Document everything. The institutional map, the legal resources, and the notes from your first institutional contact become part of the shared reference material that grows across these chapters.

Field journal: Record the institutional map, noting which institutions

the network has engaged and which remain to be explored. File the legal awareness materials alongside them. And note what the mapping surfaced about your coordination's durability. Down Home NC persists because its infrastructure belongs to the places it serves. Georgia's coalition produced extraordinary results and left nothing permanent. Which does your coordination more closely resemble — and what would need to change to ensure that what you're building belongs to the people who built it? That question, and whatever the institutional mapping turned up about ongoing coordination with existing organizations, connects to the next chapter's focus on sustaining what you've started.

Summary

Your network operates within an existing landscape of institutions, laws, and geography. Institutions can absorb grassroots energy through channeling, inclusion without power, and salience control — structural dynamics, not malicious intent. The complementary partnership model (engaging institutions as partners, not subordinates) preserves your network's autonomy. Legal awareness — assembly rights, public records, government meeting access — is civic infrastructure your network needs. Rural networks face different but not lesser terrain, with deep organizing traditions and civic infrastructure that urban-centric frameworks often overlook.

Action Items

- Map institutional landscape at a joint meeting using the six-factor assessment
- Make one deliberate institutional contact as a network
- Build a state-specific legal awareness file (ICNL tracker, ACLU guides, NLG chapter, local legal aid)
- Conduct a 30-minute legal orientation at a joint meeting
- File institutional map and legal resources in the field journal

Case Studies & Citations

- **Philip Selznick / TVA** — *TVA and the Grass Roots* (1949). Documented institutional co-optation through channeling, inclusion without power, and salience control.
- **Amanda Tattersall** — *Power in Coalition*. Complementary partnership model for grassroots-institutional engagement.
- **Cowboy Indian Alliance** — Ranchers and tribal communities maintaining distinct organizational structures while coordinating on Keystone XL opposition. Complementary partnership in practice.
- **Down Home North Carolina** — Founded 2017. County-based chapters across 25 rural NC counties. 600,000+ doors canvassed across 2020 and 2022 cycles. Permanent infrastructure rooted in place.
- **Georgia 2020 Election Protection Coalition** — Ten organizations, specialized division of labor, 800,000 new voters registered. Fair Fight and New Georgia Project both closed by 2025. Infrastructure dependent on external funding and charismatic leadership.

- **ICNL US Protest Law Tracker** — International Center for Not-for-Profit Law. State-level legislation affecting protest rights, assembly, and civic action.
- **National Freedom of Information Coalition** — State-by-state public records guides, template request letters, fee waiver guidance.
- **National Lawyers Guild** — Chapter locator at nlg.org. Legal observer trainings for community groups.
- **ACLU Know Your Rights guides** — Free, multilingual guides covering demonstrations, police encounters, and the right to record.

Templates, Tools & Artifacts

- **Institutional Mapping Framework** — Six-factor assessment: name/function, constituency, overlap, engagement history, opportunity, co-optation risk
- **Legal Awareness File** — State-specific compilation of protest law tracker results, ACLU guides, NLG contacts, local legal aid organizations

Key Terms

- **Complementary partnership** — An institutional engagement model where grassroots networks and institutions collaborate on specific shared goals while maintaining separate identities, structures, and autonomy.
- **Channeling** — An institutional dynamic where grassroots energy is redirected into institutional processes that serve the institution's legitimacy rather than the community's priorities.
- **Co-optation** — The structural absorption of grassroots opposition through the appearance of inclusion without the transfer of actual decision-making power.
- **Density bias** — The tendency of organizing literature and frameworks to assume urban institutional density, overlooking the distinct civic infrastructure and organizing traditions of rural and exurban communities.

—

Chapter 32

What Holds When It's Hard

Something came up during your institutional mapping or your first institutional contact. Maybe it was a pace disagreement — one group wanted to engage a local organization immediately, the other wanted to wait until the network felt more established. Maybe it was a discovery that challenged your assumptions — an institution you expected to be an ally turned out to have interests that conflict with yours, or a relationship that seemed promising produced friction when the actual conversation happened. Maybe it was simpler than that. Maybe someone on one group's spoke just said, at a coordination meeting, "I'm not sure this is worth the effort."

That's the question underneath this chapter. Not whether the skills work — you've practiced governance, mapped landscapes, coordinated joint actions. The question is whether the overhead of coordination is sustainable. Whether the meetings, the debriefs, the slow consent process, the energy it takes to maintain a relationship between autonomous groups — whether that's a good use of the limited time and energy your members have.

The documented record answers that honestly: coordination breaks networks. Not opposition. Not infiltration. Not lack of resources. The friction of sustained coordination — the meetings that run long, the disagreements that don't resolve cleanly, the slow accumulation of exhaustion in the people who carry the coordination load — is what kills most multi-group efforts. The Women's March mobilized the largest single-day protest in U.S. history and couldn't sustain its coalition for three years. Sunrise grew from a handful of hubs to over 500 and saw roughly 80% go inactive. These weren't failures of vision or commitment. They were structural failures — the absence of mechanisms to handle the friction that coordination inevitably produces.

This chapter is about those mechanisms. Conflict resolution between groups, sustainability at network scale, and the structural question of whether your network is ready to grow. The throughline is that friction and burnout

are design problems, not motivation problems. The structures that survive them are documented.

What Breaks Networks

The research on coalition failure converges on a consistent pattern: the conflicts that destroy multi-group coordination are almost never about values. They're about pace and priority. One group wants to move faster. The other isn't ready. One group thinks the network should focus on housing. The other thinks school board accountability is more urgent. Both care about civic engagement. Both showed up to coordinate. The disagreement isn't about why — it's about how and when.

Inside your group, you learned that conflict is personal and relational. The groan zone. Someone's feelings are hurt, someone feels unheard, the facilitator guides the group through it using the tools you built — ground rules, the consensus spectrum, NVC "I" statements. Between groups, conflict operates differently. It's structural. The disagreement isn't between two people who know each other well. It's between two groups with different internal cultures, different risk tolerances, different senses of urgency, and different relationships to the community. Your three-step escalation from the coalition agreement — goals versus methods, compatible versus incompatible interests, agree to disagree — handles many of these. But there's a harder version of the problem: what happens when the escalation itself becomes the friction?

The Women's March is the sharpest illustration. Four co-chairs held concentrated authority over a coalition of more than 550 partner organizations. When an accountability crisis surfaced — co-chair Tamika Mallory's association with Louis Farrakhan and the ensuing antisemitism controversy — the coalition had no mechanism to address it. No escalation protocol. No decision domains that separated the co-chairs' personal conduct from the coalition's direction. No way for the 550 organizations to force action. Co-founder Teresa Shook had to resort to a Facebook post to call for resignations. By the time three of the four co-chairs departed in September 2019, partner organizations had dropped from 550 to roughly 200. State chapters had dissolved. The coalition that mobilized millions of people couldn't sustain itself through one unresolved internal conflict.

The lesson isn't that the underlying disagreement was too hard. It's that no structure existed to process it. Georgetown historian Michael Kazin identified the deeper problem: every broad progressive coalition he studied that survived was focused on a single issue, creating a basis for unity that the Women's March's multi-issue identity couldn't provide. But single-issue focus isn't the only solution. The alternative is explicit governance — the tools you already have — applied before the crisis arrives.

Indivisible faced a version of the same challenge and survived it. When local-national tensions surfaced — local groups telling researchers "We don't get any resources from them. We get demands from them" — the statewide coordination bodies served as a mediating layer. Not controlling local groups, not representing the national organization. Absorbing friction that would otherwise have cascaded directly between local and national, where the power imbalance would have made resolution impossible. The statewide coordinators didn't resolve the tension. They created a space where it could be named, heard, and addressed incrementally — regular calls, shared working groups, elected representatives from each congressional district. The middle tier made the friction productive rather than destructive.

Your network's coordination structure — the spokes council, the liaison model, the decision domains — already contains the bones of a mediating structure. The question is whether you have a protocol for when those structures aren't enough.

Peer Mediation

When two groups in a network reach an impasse the three-step escalation can't resolve, a third party can help. Not a judge — a facilitator. Someone from outside the dispute whose role is to help the groups see the disagreement clearly, not to decide who's right.

If your network has a third group, the mediator comes from there. If not, consider an institutional contact from your landscape mapping — someone both groups trust, who understands your coordination but isn't part of either group's internal dynamics. The mediator doesn't need training in formal conflict resolution. They need the ability to listen without taking sides and to ask the questions the disputing groups have stopped asking

each other.

Peer Mediation Protocol

Before the session. The mediator meets briefly with each group separately — fifteen minutes, not an hour. The purpose is to understand each group's position, their core concern, and what outcome they'd consider acceptable. The mediator is looking for the gap: where does each group think the disagreement lives? Often, the groups have different theories about what they're actually fighting about. That gap is the mediator's starting point.

Opening. All parties together. The mediator sets three ground rules: each group speaks through one representative (their spoke or someone they designate), the representative describes their group's position and concern without characterizing the other group's motives, and no one interrupts. The mediator restates each position to confirm understanding before moving forward.

The diagnostic question. The mediator asks: is this disagreement about goals, methods, pace, or something else? The groups may disagree even about this — one group thinks it's about pace, the other thinks it's about values. The mediator's job is to surface that secondary disagreement, because it's often the real one. A conflict that looks like it's about whether to engage with the school board might actually be about how much public visibility the network can tolerate. A conflict about pace might actually be about capacity — one group has more bandwidth than the other and interprets caution as reluctance.

The resolution spectrum. Not every disagreement needs resolution. The mediator helps the groups identify where this one falls: Does it require a shared decision? (If so, return to the consent process with the mediator facilitating.) Can the groups pursue different approaches simultaneously without conflict? (If so, name the boundary and document it.) Is this a disagreement the network needs to hold as productive tension — an ongoing difference in perspective that informs rather than obstructs? (If so, name it explicitly. Unnamed tension becomes resentment. Named tension becomes awareness.)

Closing. The mediator summarizes what was clarified, what was decided, and what remains unresolved. Both groups confirm the summary is accurate. The outcome is documented in the field journal — not as a verdict, but as a record of what the network learned about itself.

The protocol is deliberately low-ceremony. Thirty minutes to an hour. No formal training required. The mediator's authority comes from their position outside the dispute, not from expertise. The practice of mediation — even when no real conflict exists — builds the muscle the network will need when a real one arrives. That's why the challenge includes a simulation even if your coordination is currently smooth. It won't always be.

What Sustains Networks

The documented record on network failure converges on a single finding: burnout is the most common cause. Not opposition. Not disagreement. Exhaustion. And the research is equally clear that burnout is structural, not personal. When someone burns out, examine the structure, not the person.

The COVID-era mutual aid research documented the pattern precisely: a 75% activity drop within three months of formation in most volunteer networks. Not because volunteers stopped caring. Because the infrastructure couldn't support sustained effort — unclear expectations, invisible workload distribution, no rotation of high-burden roles, and no distinction between the pace that gets something launched and the pace that keeps it running.

Your network faces this at a different scale. The coordination overhead — spokes council meetings, liaison communication, joint actions, institutional engagement — sits on top of everything your groups are already doing internally. If the coordination burden falls disproportionately on a few people, those people will burn out. And when they do, the network loses not just their energy but the institutional knowledge they carry — the relationships, the context, the understanding of how the coordination actually works.

The structural interventions are documented. None of them are complicated. All of them require deliberate implementation.

Rotating coordination roles with explicit descriptions and term limits. You're already rotating the spoke role. Extend the principle to every coordination function — whoever facilitates spokes council meetings, whoever maintains the liaison channel, whoever tracks the coalition agreement and the decision domain map. Write the role descriptions. Set the rotation

schedule. Monthly or quarterly, depending on the role's weight. When someone steps out of a role, they brief their successor. The rotation ensures no one becomes indispensable, and the briefing ensures continuity.

Regular workload check-ins. Not "how are you feeling?" — that's a personal question and gets personal answers. "How many hours did coordination take this month? How does that compare to what you expected? Is the distribution across your group roughly even?" The questions are structural and the answers are actionable. If one person is carrying twice the coordination burden, that's a design problem with a design solution: redistribute, simplify, or pause something.

The crisis-pace / sustaining-pace distinction. Some periods require intensity — a joint action is approaching, an institutional relationship needs immediate attention, an external event demands rapid coordination. That's crisis pace, and it works for weeks, not months. Sustaining pace is the baseline — the coordination rhythm the network can maintain indefinitely without anyone's other commitments suffering. The network needs to know which pace it's operating at, name it explicitly, and switch deliberately. The dangerous pattern is crisis pace that never ends — the initial energy of coordination masking an unsustainable rhythm until people start disappearing without explanation.

Explicit permission to rest. This sounds simple. It's structural. adrienne maree brown's formulation is that rest isn't a reward for work — it's a condition for sustained capacity. For your network, this means: it is acceptable for a group to reduce its coordination participation for a period. It is acceptable for a spoke to say "my group needs a quieter month." The network absorbs this without treating it as abandonment. Build this expectation into the coalition agreement. Name it before anyone needs it.

Network Health Check

At your next joint meeting — and at regular intervals afterward — run a structured assessment. Not a survey. A facilitated conversation, thirty minutes, with these questions:

How is the coordination workload distributed across groups? Within each group, who carries the coordination burden? Is anyone doing more than they committed to? Are the rotating roles actually rotating, or has rotation stalled?

What pace are we operating at — crisis or sustaining? Is that pace delib-

erate, or did we drift into it? If crisis pace: what's the timeline for returning to sustaining pace? If sustaining pace: is it actually sustainable, or are people white-knuckling it?

What's working in the coordination that we should keep doing? What's creating friction that we should redesign? What should we stop doing entirely?

Is anyone close to stepping back? Not as a guilt question — as a planning question. If the answer is yes, what would make continuation possible? If the answer is still yes, how does the network absorb that transition?

Document the answers. Compare them to the previous health check. The trend matters more than any single data point. A network where workload distribution is improving and pace is stabilizing is healthy regardless of where it started. A network where the same person has been the primary coordinator for three consecutive health checks has a single point of failure that needs addressing.

What Changes at Three Groups

Some networks, by this point, will have connected with a third group. Others won't — and that's not a failure. Your network's pace is determined by the relationships available and the coordination capacity you've built, not by a curriculum's timeline.

But the research shows something worth naming about what changes structurally when a third group joins. It's not just "more people." It's a qualitative shift in the network's properties.

At two groups, every relationship is bilateral. If the relationship between your groups deteriorates, the network is over. There's no redundancy, no alternative pathway, no one to mediate. The network is the relationship, and the relationship is the network.

At three groups, triangulation becomes possible. If Group A and Group B disagree, Group C can mediate — not because C has authority, but because C has relationships with both and a perspective outside the dispute. That's the peer mediation protocol above, made possible by structure rather than improvisation. If one group needs to step back for a month, the other two continue coordinating. The network survives the absence of any single group. Distributed specialization becomes possible — different groups de-

velop different strengths, and the network can deploy the right group for the right task.

Network science calls this triadic closure. The practical implication is simpler: a three-group network is qualitatively more resilient than a two-group coordination. Two is a partnership. Three is a network.

If your network is ready, the first-contact protocol from the opening fieldbook chapter still applies. Behavioral recognition. Observation before approach. Graduated trust. The boundary-spanner role you developed — someone with connections in multiple spaces — is your bridge. The spokes council expands by one seat. The coalition agreement and decision domains get renegotiated to include the new group's perspective. The governance structures you've built are designed for this — consent-based, adaptable, documented.

If your network isn't ready, that's the right answer. A two-group coordination that's sustainable and healthy is more durable than a three-group network that's overstretched. Deepen the institutional relationships from the last chapter instead. Growth is not the only measure of progress.

The Sunrise Movement illustrates what happens when growth outpaces governance. Founded in 2017, the organization grew from a handful of local hubs to over 500 in four years, put the Green New Deal on the national agenda, and staged actions that redefined climate politics. It also nearly destroyed itself.

The most revealing account comes from co-founders William Lawrence and Dyanna Jaye, who published a three-part self-reflection in *Convergence Magazine* in 2022. Their central admission: the founding team created a centralized nonprofit serving as a command center while telling hubs they were "fully autonomous." Lawrence and Jaye wrote that this was technically true — hubs could organize however they wanted, choose their own actions, set their own priorities. But it contained what they called "a lie of omission." Fundraising, press, and strategy were controlled by a centralized leadership of about ten people, including seven co-founders. And because, as they wrote, left activists are suspicious of hierarchy, the leadership worried their centralized body wouldn't stand up to scrutiny — so they just didn't talk about it much.

The contradiction built pressure through several phases. A fellowship program placed over 70 young organizers on minimal stipends across five swing states, creating class tensions with salaried staff. The staff expanded

from a dozen in 2018 to over 50 in 2019 and over 100 in 2020, and adopted corporate management techniques that shifted the internal culture. Hub leaders increasingly demanded transparency and democratic governance. The gap between the stated structure and the actual structure widened until it became undeniable.

By late 2023, the decline was dramatic. A democratization vote in July 2022 drew only about 700 votes nationally — from a movement that once had a universe of 80,000 supporters. Active hubs had dropped to fewer than 100 from a peak above 500. The organization that transformed climate politics couldn't sustain its own internal coordination.

I'm including this case at length not because Sunrise failed where others succeeded — every organization in these notes' case studies struggled with similar tensions. I'm including it because the founders named the failure with extraordinary honesty, and their diagnosis is the one that matters most for your network. Hidden hierarchy isn't a moral failure. It's a structural risk that any coordination faces, including yours. The moment one person or one group is doing more coordinating than others without that imbalance being visible and rotatable, you're building the same contradiction Sunrise built. Not out of bad faith. Out of convenience, urgency, and the natural tendency for capable people to take on more than their share.

Lawrence and Jaye's conclusion is worth carrying forward: movements need democratic governance with representative leadership, open strategic dialogue, and equal standing of all members. That's a description of what the spokes council, the decision domains, and the coalition agreement are designed to provide. The structures aren't bureaucracy. They're the immune system.

In Lewis Carroll's *Alice's Adventures in Wonderland*, the Queen of Hearts governed by a single principle: agreement or execution. "Off with their heads!" for any disagreement, any question, any challenge to the Queen's authority. Her court followed rules — elaborate, arbitrary, changeable rules — but the rules existed to serve the Queen's power, not to govern fairly. The croquet game had rules that changed whenever Alice was winning. The trial had procedures that existed to produce a predetermined verdict.

Alice's intervention was simpler than rebellion. She asked questions. "Why?" and "Who cares?" and, finally, "You're nothing but a pack of cards." The governance that couldn't tolerate questioning collapsed the

moment someone questioned it. The governance that survives — consent-based, transparent, accountable — is the kind that welcomes the questions. Not because questioning is comfortable, but because governance that can't handle questioning isn't governance. It's control.

Your network's coordination structures are designed to be questioned. The health check is a questioning mechanism. The mediation protocol exists because disagreements deserve structured attention, not suppression. The rotating roles ensure that no one holds enough accumulated authority to avoid accountability. The coalition agreement is revisable by consent — it changes when the network's reality changes. The structures hold not because they're rigid but because they're honest.

Challenge

Three components, adapted to where your network is.

Part 1 — Conduct a network health check. At a joint meeting, run the structured assessment described above. How is the coordination workload distributed? What pace are you operating at? What's working and what isn't? Is anyone close to stepping back, and what would the network need to absorb that transition? Document the results and compare them to any previous assessments. If this is your first health check, establish the baseline.

Part 2 — Practice the peer mediation protocol. Even if no real conflict exists, run a simulation. Pick a plausible scenario — the groups disagree about the pace of growth, or about whether to engage with a specific institution, or about how public to be about the network's existence. If you have a third group, designate a mediator from that group. If not, ask a trusted institutional contact or run the exercise with someone from one group mediating a hypothetical dispute between the other group's representatives. Walk through the full protocol: separate preparation, opening statements, diagnostic question, resolution spectrum, documented outcome. The practice builds the muscle before it's needed.

Part 3 — If ready, explore a third-group connection. Using the behavioral recognition and first-contact protocol from Chapter 27. The boundary-spanner role applies — someone with connections in spaces where other organized groups might be found. If a third group isn't available or your network isn't ready, deepen existing institutional connections instead. Use the

institutional map from the last chapter to identify one relationship worth developing further. Growth and depth are both progress.

Field journal: Record the health check results — workload distribution, current pace, what's working, what needs redesign. Note the mediation simulation outcome: what felt natural, what felt forced, what would you do differently in a real dispute? If you made contact with a potential third group, record the observation notes using the same format as Chapter 27's first-contact protocol. And note what surfaced during the health check or the mediation practice that surprised you — a capability you didn't know the network had, a vulnerability you hadn't named, a pattern that only becomes visible when you look at the coordination as a whole rather than from inside any single group. That observation — what the network can do that none of its groups can do alone — connects to what comes next.

Summary

Coordination friction — not opposition or lack of resources — is the primary cause of network failure. Conflicts between groups are typically about pace and priority rather than values. When the coalition agreement's three-step escalation isn't enough, a peer mediation protocol provides structured third-party facilitation. Sustainability requires structural interventions: rotating coordination roles, regular workload check-ins, distinguishing crisis pace from sustaining pace, and explicit permission to rest. At three groups, a network gains qualitative resilience through triadic closure — redundancy, mediation capacity, and distributed specialization.

Action Items

- Conduct a network health check at the next joint meeting
- Practice the peer mediation protocol (simulation if no real conflict exists)
- Review and update the coalition agreement to include rest provisions and pace-naming
- If ready, explore third-group connection using Chapter 27's first-contact protocol
- Document health check baseline in the field journal

Case Studies & Citations

- **Women's March (2017–2019)** — 550+ partner organizations. Four co-chairs with concentrated authority. No governance mechanism for internal accountability crisis. Three of four co-chairs departed September 2019. Partner organizations dropped from 550 to ~200. Case referenced in Chapter 30; extended here for conflict-resolution analysis.
- **Michael Kazin** — Georgetown historian. Finding that surviving progressive coalitions tend to be single-issue focused.
- **Indivisible** — Statewide coordination bodies as mediating layer between local

groups and national organization. Regular calls, shared working groups, elected representatives from congressional districts.
- **COVID-era mutual aid research** — 75% activity drop within three months of formation in most volunteer networks. Burnout as structural, not personal, failure.
- **adrienne maree brown** — Rest as condition for sustained capacity, not reward for work.
- **Sunrise Movement** — Founded 2017. Grew from a handful of hubs to 500+. Co-founders William Lawrence and Dyanna Jaye, "Understanding Sunrise" three-part self-reflection, *Convergence Magazine*, 2022. Key findings: centralized non-profit with "fully autonomous" hubs constituted "a lie of omission"; leadership of ~10 people including 7 co-founders controlled strategy while hubs were told they were self-directing; staff grew from 12 (2018) to 50+ (2019) to 100+ (2020); fellowship placed 70+ organizers on minimal stipends creating class tensions; democratization vote (July 2022) drew ~700 votes from 80,000-person universe; active hubs dropped to fewer than 100 by late 2023.
- **Triadic closure** — Network science concept. A three-group network is qualitatively more resilient than a two-group partnership: redundancy, mediation capacity, distributed specialization.

Templates, Tools & Artifacts

- **Peer Mediation Protocol** — Pre-session separate meetings, opening ground rules, diagnostic question, resolution spectrum, documented outcome
- **Network Health Check** — Structured 30-minute assessment: workload distribution, pace identification, friction/success inventory, transition planning
- **Sustainability Framework** — Rotating roles with descriptions and term limits, structural workload check-ins, crisis/sustaining pace distinction, explicit rest provisions

Key Terms

- **Crisis pace vs. sustaining pace** — The distinction between the intensity of coordination that works for short periods (weeks) during urgent activity and the baseline rhythm a network can maintain indefinitely.
- **Triadic closure** — The network science principle that a three-node network is qualitatively more resilient than a two-node partnership, enabling redundancy, mediation, and distributed specialization.
- **Peer mediation** — A structured process where a third party outside a dispute facilitates clarification and resolution between two groups, using position rather than expertise as the source of authority.
- **Hidden hierarchy** — Informal, unaccountable leadership that exists in ostensibly structureless or distributed organizations, identified by Jo Freeman and illustrated by the Sunrise Movement case study.

—

Chapter 33

More Than the Sum

Your health check or your mediation practice surfaced something. Maybe it was during the workload assessment — someone listed the things the network handles routinely now, and the list was longer than anyone expected. Maybe it was during the mediation simulation — a third group offered a perspective that neither of the disputing groups had considered, and the resolution came from that outside angle. Maybe it was simpler. Someone said "if we'd tried this six months ago with just our group, we couldn't have done it," and the room agreed without discussion.

That's the observation underneath this chapter. Your network can do things none of your groups can do alone.

The documented record on network coordination identifies specific properties that emerge when autonomous groups coordinate past a threshold of sustained practice — properties that don't exist inside any individual group, no matter how capable. You've built those properties. This chapter names them and provides the civic infrastructure that makes them operational.

What the Network Already Is

Three properties. You've already demonstrated each of them, whether or not you used these words.

Resilience. If one group goes quiet for a month — burnout, personal crises, a member's family emergency — the network continues. The coordination doesn't collapse. The other groups carry the liaison relationships, maintain the institutional contacts, keep the civic monitoring going. When the resting group returns, the continuity is there. This isn't redundancy for its own sake. It's the structural difference between a partnership and a network. Your health check tested this: if any single group disappeared for

thirty days, would the network's core functions survive? If yes, you have resilience. If no, you have a single point of failure to address.

Distributed capability. Different groups develop different strengths. One group is good at facilitation and runs the coordination meetings. Another has someone skilled at public records requests. A third has the strongest institutional relationships. The network can deploy the right group for the right task — not because someone assigned specializations, but because practice revealed them. The mediation simulation demonstrated this: the mediating group brought a perspective the other two couldn't generate internally. That's distributed capability in action. No group has to be good at everything because the network is.

Rapid coordination. When something happens in your community that requires attention — a concerning vote at city council, a sudden infrastructure decision, an institution acting against community interests — you don't need to build coordination from scratch. The liaison channel exists. The spokes council meets regularly. The decision domains are mapped. The coalition agreement defines how you decide together. The infrastructure for collective response already exists. It just needs activation, not construction.

The documented record shows these properties consistently in networks that survive their first year. The Election Protection Coalition coordinates 42,000 volunteers across 300-plus partner organizations through a structure built on exactly these principles — distributed responsibility across specialized working groups, enough governance to coordinate without enough to control, and shared information infrastructure that any partner can access. The Coalition didn't build that capacity during election season. It maintained it year-round, activating different components as the calendar required.

Your network operates at a fraction of that scale. The architecture is the same.

Civic Monitoring

The network's coordination infrastructure has one more function — one I came to see as among the most consequential for long-term civic health. You can watch.

Not surveillance. The opposite. Democratic governance depends on informed constituents who know what their government is doing. The mechanisms for this are public, legal, and underused. Your network — with distributed capability, regular coordination, and shared information channels — is structurally suited to do what most individual citizens can't sustain alone: consistent, informed civic monitoring.

The League of Women Voters has operated an Observer Corps since the organization's founding in 1920. The model is straightforward: trained volunteers attend public government meetings, take structured notes, and report what they observed to a broader membership. The observers don't testify. They don't lobby. They don't protest. They watch, record, and share. The power is in the consistency — when public officials know that informed citizens attend every meeting and document the proceedings, the proceedings change. Research on municipal governance transparency consistently finds that regular observation by organized citizens correlates with better record-keeping, more public comment opportunities, and fewer decisions made in ways that circumvent public notice requirements.

Your network can adapt this model without affiliating with the LWV or any other organization. Here's the framework:

Identify the relevant bodies. City council, county commissioners, school board, planning and zoning boards, utility commissions — the public bodies whose decisions most directly affect your community. Your institutional map from the landscape chapter is the starting reference. Most of these bodies hold meetings on published schedules, often monthly or biweekly.

Assign the rotation. Each group takes responsibility for specific meetings on a rotating basis. Group A covers city council this month; Group B covers school board; Group C covers planning commission. Next month, rotate. The rotation prevents any single group from developing a narrow institutional focus and ensures multiple groups develop familiarity with multiple bodies. The spoke for each group coordinates the assignment. One person per meeting is sufficient — two if the meeting covers a known contentious issue.

Use a simple observation template. The observer records: the date, body, and location. Who was present (members, staff, public attendees). What was on the agenda versus what was actually discussed. What decisions were made and how (unanimous, split vote, tabled). What public comment was offered. What surprised the observer — the most subjective

and often most valuable field. Share the completed template through the liaison channel after each meeting.

Discuss at coordination meetings. The spokes council's regular meeting includes a standing item: civic monitoring updates. Each group's representative shares anything notable from the meetings they observed. The network builds a cumulative picture of local governance — patterns, recurring issues, emerging decisions — that no individual attending occasional meetings could assemble.

Decide whether and how to engage. Observation is the foundation. Engagement is the network's choice. If the monitoring reveals an issue the network wants to address — a budget allocation, a policy proposal, a pattern of closed-door decisions — the coalition agreement's decision domains determine how the network responds. Some issues might warrant public comment. Others might warrant a FOIA request. Others might simply warrant continued observation. The monitoring informs the decision. The decision belongs to the network.

FOIA and Public Records

The Freedom of Information Act at the federal level and state-level equivalents — usually called public records laws or open records acts — give any person the right to request government documents. The specifics vary by state, but the principle is consistent: government records are public unless a specific exemption applies, and the burden of justifying withholding falls on the government, not the requester.

Filing a public records request is one of the most underused civic tools available to ordinary citizens. It requires no lawyer, no organizational affiliation, no special standing. The process is administrative, not adversarial — you're asking for documents the government is legally required to provide.

For your network, a public records request serves two purposes. First, it produces information — budget documents, correspondence, meeting minutes, inspection reports, enforcement records — that informs the network's understanding of local governance. Second, the practice of filing teaches the network how the process works, which makes future requests faster and more targeted.

Choosing what to request. Start with something specific to an issue your civic monitoring has surfaced. Broad requests ("all records related to housing") produce delays and mountains of paper. Targeted requests ("inspection reports for [specific address or facility] between January and June 2025") produce usable documents. The civic monitoring observations are your targeting mechanism — they tell you which decisions, which bodies, and which timeframes matter.

Filing the request. Most jurisdictions accept requests by email. Some have online portals. The National Freedom of Information Coalition and state press associations maintain guides to each state's specific process, timelines, and fee structures. Filing on behalf of an organization (your network, described in whatever terms you choose) can strengthen fee waiver arguments — journalists and organizations acting in the public interest often qualify for reduced or waived fees.

What to do with what comes back. Share it through the liaison channel. Discuss it at the spokes council. The documents themselves may be unremarkable — routine budget allocations, standard inspection reports. Or they may reveal patterns: spending priorities that don't match public statements, enforcement gaps, decisions made without the public engagement the law requires. Either outcome is informative. The network's civic monitoring now includes not just observation of public meetings but access to the documentary record behind them.

Communication at Three-Plus Groups

Your liaison model from the earlier chapters scales naturally. Each group has a designated liaison — the spoke — who participates in the coordination channel. The coordination channel is the single shared communication space for inter-group matters. The spokes council meets regularly.

At three-plus groups, one structural addition makes the coordination sustainable: a standing coordination meeting with a predictable cadence. Monthly is the recommended default — more frequent if the network is actively coordinating on a time-sensitive matter, less frequent during periods of lower activity. The meeting has a consistent format: civic monitoring updates, active coordination items, upcoming decisions requiring consent, and any concerns or proposals from individual groups.

The meeting replaces the ad-hoc communication that works at two groups but fragments at three or more. Instead of multiple bilateral conversations between spokes — which increases quadratically with each new group and produces information asymmetries — the standing meeting puts every group's representative in the same conversation at the same time. What's decided is documented. What's pending is tracked. What's observed through civic monitoring is shared.

Keep the structure minimal. One channel. One regular meeting. Clear escalation for urgent matters (defined in the coalition agreement). The network should add structure only when the existing structure demonstrably fails, not in anticipation of complexity that may not arrive.

In the first season of *Squid Game*, 456 players are under total surveillance — cameras in every room, masked guards monitoring every corridor, the Front Man watching from a screen. The players have no privacy, no information about the game's design, no way to observe the people making the rules. The power asymmetry is absolute: the game watches the players, and the players can't watch the game.

But during the sleep periods — the unstructured time between rounds — the players organize. They form alliances. They share observations. They develop strategies based on what each person noticed from their different vantage point during the games. No individual player sees the whole picture. Together, they assemble something closer to it. The organizing doesn't happen because someone gave them a protocol. It happens because distributed observation, shared through trust relationships, is the natural response to opaque power.

The VIPs — the wealthy spectators betting on outcomes from a luxury viewing room — represent the inverse. They have total information and no accountability. They watch without being watched. Their decisions shape the game, and the players have no mechanism to observe, question, or influence those decisions.

Civic monitoring is the structural answer to that asymmetry. Not total — democratic governance will always have information advantages over citizens. But the gap between total opacity and informed observation is the gap between governance that serves the governed and governance that serves itself. The Observer Corps model, public records requests, consistent attendance at public meetings — these are the mechanisms by which ordinary people build their own eyes and ears. The question *Squid Game*

poses visually — who watches, and who is watched? — is the question every democracy answers through its transparency infrastructure. Or fails to answer.

Your network's civic monitoring doesn't require surveillance of anyone. It requires showing up to meetings that are legally public, requesting documents the law entitles you to receive, and sharing what you learn with people who care about the same community. That's not radical. It's the minimum viable practice of informed self-governance.

Challenge

Two components.

Part 1 — Start a civic monitoring rotation. Using the framework above: identify the two or three government bodies most relevant to your community. Assign groups to attend their next meetings on a rotating basis. Each observer uses the simple template — date, body, attendance, agenda versus discussion, decisions, surprises. Share the completed observations through the liaison channel. Discuss the findings at your next spokes council meeting. This is the beginning of a practice, not a one-time exercise. The rotation should be sustainable — monthly observation of two or three bodies is more valuable than a burst of coverage that fades after a month.

Part 2 — File a public records request. Choose a specific issue that your civic monitoring or your community knowledge has surfaced. Use your state's public records process to file a targeted request. The filing itself is the primary learning objective — understanding the process, the timelines, the fee structures, and the specificity required. Share what you file and what you receive through the liaison channel. If the response reveals something worth discussing, bring it to the spokes council.

Field journal: Record the civic monitoring observations — what you saw, what surprised you, what patterns you noticed across different public bodies. Document the public records request: what you requested, the process, what came back. Note what the monitoring or the records revealed that the network didn't previously know — a pattern in local decision-making, a gap between public statements and documented actions, an issue that affects your community more directly than you'd realized. That

finding — whatever it is — connects to the next chapter. What you're monitoring, and what it reveals, will inform the conversation about what holds your network together beyond the original reason you connected.

Summary

Your network has three structural properties no single group has: resilience (it continues when one group rests), distributed capability (different strengths for different tasks), and rapid coordination (collective-response infrastructure exists and only needs activation). These make civic monitoring—meeting attendance, structured notes, and public records requests—sustainable for your network where individuals can't. The Observer Corps model, with rotating assignments and shared reporting, gives you eyes on community decisions; public records requests open the documentary record behind them. At three-plus groups, add one structure: a standing coordination meeting on a predictable cadence, replacing bilateral conversations that fragment as the network grows.

Action Items

- Identify the two or three government bodies most relevant to your community and assign the first month's civic monitoring rotation
- Create or adapt the observation template (date, body, attendance, agenda vs. discussion, decisions, surprises)
- Add civic monitoring updates as a standing item in your spokes council meetings
- File one targeted public records request based on an issue your monitoring or community knowledge has surfaced
- Review your liaison channel and coordination meeting cadence — is the structure still minimal and functional at your current size?

Case Studies & Citations

- **Election Protection Coalition** — Led by the Lawyers' Committee for Civil Rights Under Law, co-led by Common Cause. 300+ national, state, and local partner organizations. 42,000+ volunteers. Multi-language hotlines (English, Spanish, Chinese/Vietnamese/Korean/Bengali/Hindi/Urdu/Tagalog, and Arabic). Structure: distributed responsibility across specialized working groups, year-round maintenance with seasonal activation.
- **League of Women Voters Observer Corps** — Operating since the LWV's founding in 1920. Trained volunteers attend public government meetings as silent observers, document official attendance, compliance with sunshine laws, issues discussed, and process concerns. Observers do not testify, lobby, or protest. Reports submitted via standardized forms and published publicly. (LWV Education Fund, *Observing Your Government in Action — A Resource Guide*)
- **Freedom of Information Act (FOIA)** — Federal law (5 U.S.C. § 552) establishing the public's right to request records from federal agencies. State equivalents exist in all 50 states under varying names (public records laws, open records acts, sunshine laws). The National Freedom of Information Coalition maintains state-by-state guides to processes, timelines, and fee structures.

Templates, Tools & Artifacts

- **Civic Monitoring Observation Template** — Date, body, location, attendance (members/staff/public), agenda vs. actual discussion, decisions and vote type, public comment, observer's surprises. Shared through liaison channel after each meeting.
- **Civic Monitoring Rotation Schedule** — Group-to-body assignment grid, rotating monthly. Spoke coordinates each group's assignment.
- **Standing Coordination Meeting Agenda** — Civic monitoring updates, active coordination items, upcoming consent decisions, group concerns and proposals.

Key Terms

- **Emergent network properties** — Capabilities (resilience, distributed capability, rapid coordination) that arise from sustained inter-group coordination and don't exist within any individual group.
- **Civic monitoring** — Systematic observation of local government through attendance at public meetings, structured documentation, and public records requests. Adapted from the League of Women Voters Observer Corps model for informal networks.
- **Public records request** — Administrative request for government documents under FOIA (federal) or state equivalents. Requires no lawyer, organizational affiliation, or special standing.
- **Standing coordination meeting** — Regular meeting of all group liaisons (spokes) with a consistent agenda, replacing ad-hoc bilateral communication that fragments at three-plus groups.

Chapter 34

Shared Principles, Separate Paths

Your civic monitoring has started surfacing patterns. The public records responses, the meeting observations, the conversations between liaisons about what they've noticed — these are producing something more than information. They're producing questions. Not questions about the data, but questions about the network itself. What are we actually coordinating toward? What holds us together beyond the shared concern that brought our groups into contact? If a new group approached us tomorrow, what would we tell them we stand for?

This chapter is about those questions. Not because they're philosophical — because they're structural. A network without shared principles isn't leaderless. It has leaders. They're just invisible.

The most important essay most organizers have never read is Jo Freeman's "The Tyranny of Structurelessness." First published in *The Second Wave* in 1972, drawn from Freeman's experience in the women's liberation movement, it identifies a pattern that has since repeated in virtually every decentralized movement the documented record contains. The pattern is this: groups that reject formal structure don't eliminate hierarchy. They make hierarchy informal, unaccountable, and invisible.

Freeman's analysis is precise. In groups without explicit structure, friendship networks become unacknowledged power structures. People with more social connections, more free time, and more shared background with other influential members accumulate informal authority. Without formal spokespersons, media selects its own representatives, creating resentment. Without defined roles, the people who do the most work accumulate the most influence — not because they sought it, but because the work requires decisions and decisions require someone to make them.

The essay is freely available online at jofreeman.com. This chapter's recommendation: read it together at a joint meeting. Discuss it as a network.

The conversation matters more than the text, because the text describes a general pattern and the conversation applies it to your specific network.

Three questions for that discussion:

Where do we already see informal hierarchy in our coordination? Not as accusation — as observation. Someone is probably doing more coordinating than others. Someone's opinion probably carries more weight. Someone's schedule probably shapes when meetings happen. Name it. Naming is not the problem. Hiding is the problem.

Where is our current structure helping us? The spokes council, the decision domains, the coalition agreement — which of these are actually functioning, and which exist on paper but get bypassed in practice? The structures that are working are worth keeping. The structures that aren't might be the wrong structures rather than unnecessary ones.

Where is structure constraining us? Is the consent-based process slowing decisions that don't need it? Are the decision domains too rigid for the situations you're actually facing? Freeman's point isn't that all structure is good. It's that hidden structure is worse than visible structure, even when the visible structure is imperfect.

Freeman proposed specific solutions: delegate authority to specific individuals for specific tasks, require those delegates to report back, distribute authority as widely as reasonably possible, rotate tasks among qualified members, ensure equal access to information, and provide equal access to resources. These aren't radical proposals. They're the structural equivalent of making the invisible visible. Your network has already implemented most of them through the governance frameworks in earlier chapters. The Freeman discussion is a diagnostic tool — a way to check whether what you built is actually functioning the way you designed it.

Freeman describes what goes wrong. The documented record also shows what holds together — across decades, across continents, without centralized control.

Alcoholics Anonymous has maintained decentralized coherence for more than ninety years across two million participants in over 180 countries. No central authority dictates what individual groups do. Each group is autonomous. What holds AA together are the Twelve Traditions — not rules, but principles that every group references and adapts to its own context.

Three of those traditions are directly relevant to your network. Tradition Two: "For our group purpose there is but one ultimate authority —

a loving God as He may express Himself in our group conscience. Our leaders are but trusted servants; they do not govern." Strip the theological language and the structural principle is clear: authority flows from the collective, not from the leaders. Leaders serve the group's decisions; they don't make them. Tradition Four: "Each group should be autonomous except in matters affecting other groups or A.A. as a whole." Autonomy has limits. Those limits are defined collaboratively, not imposed from above. And Tradition Nine: "A.A., as such, ought never be organized; but we may create service boards or committees directly responsible to those they serve." Organization is not forbidden — but it exists to serve, not to govern.

The Quaker tradition is older and makes the same structural argument differently. For more than 370 years, the Religious Society of Friends has maintained coherent practice across diverse communities through shared Testimonies — Peace, Equality, Simplicity, Truth, Stewardship — rather than creedal rules. Monthly Meetings operate autonomously but are accountable to Quarterly and Yearly Meetings. Clerks facilitate rather than direct. Decision-making proceeds by "sense of the meeting" rather than majority vote. Positions rotate on roughly three-year terms. And the Books of Discipline that guide each yearly meeting evolve as "living documents" — they're expected to change as the community's understanding deepens.

Food Not Bombs has operated since 1980 across roughly a thousand chapters in over sixty countries with three shared principles: the food is always vegan or vegetarian and free to everyone without restriction; each chapter is independent, autonomous, and makes decisions by consensus; and the organization is dedicated to non-violent direct action rather than charity. No central organization. No membership dues. No hierarchy. Anyone can start a chapter. Identity is maintained through shared name, shared principles, and shared practice — not through institutional structure.

The pattern across these organizations: loose alignment on values provides more durable coherence than rigid procedural requirements. Principles guide without commanding. They're broad enough to hold diverse communities and specific enough to guide real decisions. And critically, they're chosen by the people who live by them — not imposed from above by a board, a founder, or a curriculum.

The Sunrise Movement illustrates what the founders themselves recom-

mended as the alternative to what went wrong. You've already encountered the case in these pages — in Chapter 30, briefly, alongside the discussion of governance without consent, and at length in Chapter 32, where the hidden hierarchy and its structural costs were the central lesson. Roughly 400 of 500 hubs went inactive. The organization that transformed climate politics couldn't sustain its own coordination.

What matters for this chapter isn't the diagnosis — you've read that. It's the prescription. In their *Convergence Magazine* self-reflection, co-founders William Lawrence and Dyanna Jaye didn't just name the failure. They described what would have worked: member democracy with representative leadership, open strategic dialogue, and equal standing of all members.

Each element of that prescription maps to something concrete. Member democracy means the people doing the work have genuine decision-making power — not advisory input, not the ability to organize locally within parameters set centrally, but actual authority over the organization's direction. Representative leadership means coordinators who serve defined mandates from the people they coordinate — the spokes council model, not the command center model. Open strategic dialogue means the strategic choices are made transparently, debated collectively, and revisable by the membership — not made by a small group and announced as decisions. Equal standing means that every hub, chapter, or group has the same formal relationship to the whole — no inner circle with privileged access to resources, information, or decision-making.

The founders' prescription is, in structural terms, a description of governance through shared principles rather than imposed rules. The principles are chosen, transparent, and revisable. The leadership serves defined mandates. The strategic direction belongs to the membership. That's what the AA Traditions, the Quaker Testimonies, and the Food Not Bombs model all demonstrate at scale across decades. And it's what a shared principles document makes possible for your network — not because the document has magic properties, but because the process of writing it together forces the conversations that hidden hierarchy avoids.

In Apple TV's *Severance*, Lumon Industries' Board of Directors governs the severed floor through rules the innies didn't make, can't question, and don't understand. The Board is unseen. Its authority is absolute. Its decisions shape every aspect of the innies' working lives — what they're allowed to know, who they're allowed to talk to, what behaviors earn re-

wards and which earn corrections. The rules aren't principles. They're control mechanisms designed to look like organizational structure.

The show's central tension isn't between the innies and the Board. It's between governance imposed from above and governance chosen from below. The innies don't rebel by breaking rules. They rebel by forming relationships the system was designed to prevent — by choosing to coordinate despite a structure engineered to keep them isolated. Their resistance is structural before it's dramatic. They build trust across compartments that were meant to stay separate. They share information the system classified as forbidden. They act collectively in a space designed for individual compliance.

The Board's governance fails not because the rules are harsh but because they weren't chosen by the people who live under them. They can't be questioned, so they can't be improved. They can't be revised, so they can't adapt. They have no legitimacy beyond the power to enforce them.

Your network's principles work differently. They're written by the people who'll live by them. They're revisable by consent. They exist because the network chose them, not because someone imposed them. The difference between Lumon's Board and your network's shared principles isn't the content of the rules — it's who makes them, who can change them, and whether they serve the people they govern.

These pages recommend writing your network's shared principles at a joint meeting using a facilitated process. Not a constitution. Not bylaws. Not a mission statement drafted by a committee of two. A short document — three to seven principles — written collectively, reflecting what the network has learned about itself through the work it's already done.

The facilitation structure: four questions, discussed in sequence.

What brought our groups together? This is the origin story — not in mythological terms, but in practical ones. What specific concern, connection, or event led to the first boundary-spanner meeting? Name it concretely. Networks that lose track of their origin drift.

What holds us together beyond the original reason? The original concern may have evolved. The network may have discovered shared interests that weren't visible at first contact. The institutional mapping, the civic monitoring, the joint actions — these may have revealed common ground that the origin story doesn't capture. Name what's emerged.

What commitments do we share? Not aspirations — commitments.

What does the network actually do, and what does it refuse to do? These should be observable in practice, not just expressible in language. If a principle isn't reflected in behavior, it isn't a principle yet. It's an aspiration, and that's fine — but name it honestly.

What do we refuse to do? This is often the most clarifying question. Shared refusals define boundaries more crisply than shared aspirations. The network might refuse to endorse candidates. Refuse to share members' personal information with institutional partners. Refuse to make decisions without all groups represented. Refuse to grow faster than trust allows. The refusals tell you what the principles actually protect.

These pages provide the examples above — AA, Quakers, Food Not Bombs — as reference points, not templates. Your principles should emerge from your network's experience, not from historical models. The process of writing them together is the point. The document is the artifact of the conversation.

Keep the principles broad enough that groups with different local concerns can live by them. Keep them specific enough that a concrete decision could actually be tested against them. And treat them as a living document — revisable by the same consent-based process the network uses for other decisions. The Quakers revise their Books of Discipline regularly. In November 2023, the Zapatistas dissolved the autonomous municipal structures they'd maintained for nearly thirty years in Chiapas, Mexico, and reorganized into thousands of more localized governance bodies — Local Autonomous Governments where each community directs its own affairs, with regional coordination serving the communities rather than governing them. The reorganization came after years of critical self-evaluation and mounting external pressures, including cartel violence along the Guatemala border. Their communiqué described the new structure as placing the base at the top — communities governing the zones and regions, not the other way around. Governance is never finished. Build the expectation of evolution into the structure itself.

If your network is ready to grow, these pages provide an onboarding protocol. "Ready" doesn't mean "wants to." It means the existing coordination is healthy — the health check from the last phase shows sustainable workload distribution, the governance structures are functioning, and the network has spare coordination capacity rather than operating at its limit.

The protocol follows the same recognition-based approach from the

first chapters of Level 3. A boundary-spanner from the new group meets with liaisons from existing groups — the same first-contact protocol, the same behavioral recognition framework. The difference is that the network now has institutional memory. The shared principles document gives the new group something concrete to read and respond to before the relationship deepens. The coalition agreement, the decision domains, the liaison model — these are documented and shareable.

The onboarding sequence: boundary-spanner meetings first, establishing whether the groups' concerns and practices are compatible. A probationary coordination period — participation in one or two joint coordination meetings as observers before formal inclusion. Review and discussion of the shared principles document — not as a loyalty test, but as a conversation about fit. Does the new group share these commitments? Would they modify them? Those modifications might improve the document. And finally, a consent-based decision by the existing network about whether to formalize the connection.

The emphasis throughout is deliberate growth, not rapid expansion. The research is unambiguous on this point. Sunrise grew from a handful of hubs to over 500 in four years and lost roughly 80% of them. Indivisible spawned 6,000 groups in weeks and retained roughly a third. AA, which has grown for ninety years, builds growth into the program itself — the Twelfth Step requires helping others — but the growth happens through personal relationships, one sponsor to one newcomer, at the speed of trust.

If your network isn't ready, deepen what exists. The shared principles conversation, the Freeman discussion, the civic monitoring rotation — these strengthen the network's foundation whether or not a new group joins. Growth is not the only measure of progress.

Challenge

Three components, adapted to your network's current situation.

Part 1 — Write your network's shared principles. At a joint meeting, use the four-question facilitation process described above. Aim for three to seven principles. Write them together — not delegated to a drafting committee. Keep them broad enough for diverse groups, specific enough for real decisions, and treat the document as revisable. Document the result

and share it through the liaison channel.

Part 2 — Read and discuss Freeman's "Tyranny of Structurelessness." The full essay is freely available at jofreeman.com. Distribute it before a joint meeting. Discuss using the three diagnostic questions above: Where do we see informal hierarchy? Where is structure helping? Where is it constraining? The conversation will surface things the shared principles document should address.

Part 3 — If the network is growing, run the onboarding protocol. Boundary-spanner meetings, probationary coordination period, shared principles review, consent-based admission. If the network isn't growing, revisit the coalition agreement from Chapter 30 and update it based on everything you've learned since you wrote it. The agreement was drafted before the institutional mapping, before the joint actions, before the conflict resolution practice. It's almost certainly incomplete.

Field Journal

Two entries for the network's shared record.

First, document the shared principles themselves. This is the network's most important document — not because it's permanent, but because it represents the first time the network articulated what holds it together. Date it. Note who was present. Note any principles that generated significant discussion — the disagreements reveal as much as the agreements.

Second, note what the Freeman discussion revealed about the network's current structure. Where is informal hierarchy operating? What did the network decide to do about it — make it visible, rotate it, formalize it, or accept it as a productive asymmetry? These observations will inform the conversation in the next chapter about what you'd tell someone who's just starting this process.

The principles aren't the answer. The conversation that produced them is.

Summary

A network without shared principles isn't leaderless — it has invisible leaders. Jo Freeman's "Tyranny of Structurelessness" identifies the pattern: groups that reject formal structure make hierarchy informal and unaccountable. Three organizations demonstrate the alternative — AA's Twelve Traditions, the Quaker Testimonies, and Food Not Bombs' three shared principles — each maintaining decentralized coherence across decades through values-based alignment rather than procedural control. The Sunrise Movement's founders prescribed the same structural approach as a remedy for what went wrong in their organization. Writing your network's shared principles through a four-question facilitation process (origin, evolution, commitments, refusals) forces the conversations that hidden hierarchy avoids. If the network is ready to grow, a recognition-based onboarding protocol ensures deliberate expansion at the speed of trust.

Action Items

- Read Freeman's "Tyranny of Structurelessness" (jofreeman.com) and discuss at a joint meeting using the three diagnostic questions
- Write your network's shared principles at a joint meeting using the four-question facilitation process
- If growing: run the onboarding protocol (boundary-spanner meetings → probationary coordination → shared principles review → consent-based admission)
- If not growing: revisit and update the coalition agreement from Chapter 30 based on current experience
- Build revision into the structure — schedule a review of the shared principles document at a defined interval

Case Studies & Citations

- **Jo Freeman, "The Tyranny of Structurelessness"** — First published in *The Second Wave*, Vol. 2, No. 1 (1972). Originally delivered as a speech at the Southern Female Rights Union conference, Beulah, Mississippi, May 1970. Also published in *Berkeley Journal of Sociology*, Vol. 17, 1972–73, pp. 151–165, and *Ms.* magazine, July 1973. Freely available at jofreeman.com.
- **Alcoholics Anonymous Twelve Traditions** — Adopted 1950. Traditions 2, 4, and 9 cited. Two million+ participants, 180+ countries, 90+ years of decentralized coherence.
- **Religious Society of Friends (Quakers)** — Founded 1650s. Shared Testimonies (Peace, Equality, Simplicity, Truth, Stewardship). Monthly/Quarterly/Yearly Meeting structure. Clerks facilitate; decision by "sense of the meeting." Books of Discipline as living documents.
- **Food Not Bombs** — Founded 1980, Cambridge, Massachusetts. Roughly 1,000 chapters in 60+ countries. Three principles: vegan/vegetarian food free to all, each chapter independent and autonomous with consensus decision-making, dedicated to non-violent direct action. (foodnotbombs.net)
- **Sunrise Movement** — Founded 2017. Co-founders William Lawrence and Dyanna Jaye, "Understanding Sunrise" three-part self-reflection, *Convergence Magazine*, 2022. Prescriptive recommendations: member democracy, representative leadership, open strategic dialogue, equal standing.
- **Zapatista reorganization (November 2023)** — EZLN dissolved Rebel Zapatista Autonomous Municipalities (MAREZ) and Councils of Good Government (JBG). Replaced with Local Autonomous Governments (GAL) coordinating into re-

gional Collectives (CGAZ) and zone-level Assemblies (ACGAZ). Communiqué signed by Subcomandante Insurgente Moisés, November 6, 2023; new structure described in Ninth Part communiqué, November 13, 2023. Context: cartel violence along Guatemala border, critical self-evaluation after 30 years of autonomous governance.

Templates, Tools & Artifacts

- **Shared Principles Facilitation Process** — Four-question sequence for a joint meeting: (1) What brought our groups together? (2) What holds us together beyond the original reason? (3) What commitments do we share? (4) What do we refuse to do? Aim for 3–7 principles. Document and share through liaison channel.
- **Freeman Diagnostic Questions** — Three questions for a joint discussion after reading the essay: (1) Where do we see informal hierarchy? (2) Where is structure helping? (3) Where is it constraining?
- **Onboarding Protocol** — Boundary-spanner meetings → probationary coordination period (1–2 meetings as observers) → shared principles review and discussion → consent-based admission by existing network.

Key Terms

- **Tyranny of structurelessness** — Jo Freeman's term for the pattern in which groups that reject formal structure develop informal, unaccountable hierarchy rather than eliminating hierarchy.
- **Shared principles** — A short document (3–7 principles) written collectively by the network, reflecting commitments observable in practice. Revisable by consent. Broader than rules, more specific than aspirations.
- **Onboarding protocol** — Recognition-based process for integrating new groups into an existing network, emphasizing deliberate growth at the speed of trust rather than rapid expansion.
- **Living document** — A governing text designed to be revised as the community's understanding evolves, modeled on the Quaker Books of Discipline and the Zapatista governance restructuring.

Chapter 35

What You'd Tell Someone Starting

The shared principles conversation surfaced something these pages can't give you. When you sat together and wrote down what holds the network together — the commitments, the refusals, the history of how you found each other — you weren't referencing a curriculum. You were articulating experience. The Freeman discussion revealed where invisible hierarchy was operating and what to do about it. The four questions forced the network to decide what it actually stands for, in concrete terms, on the record. The principles document that emerged didn't come from a researcher who's never coordinated anything at this scale. It came from your network's practice.

That distinction matters for what this chapter asks you to do. Because the most important thing the network will produce isn't a joint action, a civic monitoring report, or a shared principles document. It's the thing you make for the people who come after you.

Alcoholics Anonymous has a design insight embedded in its program that closes the loop. The twelfth step — the final step in the program — requires that you help another person begin. Not as charity. Not as outreach. As completion. You haven't finished the work until you've helped someone else start it.

The insight isn't altruistic. It's structural. Teaching what you've learned forces you to understand it differently. The person explaining the first step to a newcomer discovers gaps in their own understanding that the step itself didn't reveal. The sponsor articulating why the third step matters has to decide, for themselves, why it matters — a decision that happens in the teaching, not in the initial learning. AA's reproduction mechanism doesn't just spread the program. It deepens it for the person doing the spreading.

The Highlander Center's popular education tradition arrives at the same

place from different premises. Myles Horton's conviction — the answers to a community's problems already exist within the community — isn't a motivational statement. It's a claim about where knowledge lives. Highlander didn't bring expertise to communities. It created conditions for communities to surface their own. The Citizenship Schools that Septima Clark developed and carried across the South — about a thousand of them by the time she retired in 1970 — trained local people to teach literacy and voter registration in their own communities. Clark had been fired from her teaching position in Charleston for refusing to deny her NAACP membership. She turned that loss into a program that trained an estimated ten thousand grassroots leaders. The organizers who trained at Highlander and went on to help build SNCC, to plan the Freedom Rides, to staff the Mississippi Freedom Schools — they taught what they'd just learned, in communities they belonged to, to people who trusted them because they'd done the same work.

The research confirms what both traditions discovered through practice. Near-peer teaching — where the teacher is only slightly more experienced than the learner — consistently outperforms expert instruction across domains. Peer tutoring meta-analyses show a "teacher-slightly-ahead" model producing better outcomes for both teacher and learner than either same-level collaboration or traditional expert-to-novice instruction. The mechanism is proximity: someone who struggled with the material last month remembers where the confusion lives. An expert who mastered it years ago has forgotten. And the act of teaching produces what researchers call the "protégé effect" — the teacher's own understanding deepens through the work of making it transferable. You don't fully know what you know until you try to give it away.

Your network is in the near-peer position right now. You learned these skills recently enough that the difficulty is still visible. You built these practices in a specific place, with specific people, facing specific challenges. That specificity is an advantage no general curriculum can match. A starter kit written by people who learned threat modeling six months ago and taught it to their neighbors is more useful to someone starting today than one written by a security researcher who's been doing this for twenty years.

In October 2012, Hurricane Sandy hit New York City. Within days, an informal network of Occupy Wall Street veterans mobilized under the name Occupy Sandy. They weren't disaster professionals. They were orga-

nizers who had practiced coordination, supply chains, and rapid decision-making during the Zuccotti Park encampment. The operation that emerged — roughly sixty thousand volunteers, over a million dollars in donations and supplies, direct relief in neighborhoods that FEMA and the Red Cross took weeks to reach — was widely reported as the organizational surprise of the disaster. The U.S. Department of Homeland Security later commissioned a study on Occupy Sandy's effectiveness, calling it one of the leading humanitarian groups in the response.

What was less reported was what happened after.

The veterans of Occupy Sandy didn't disband when the immediate crisis passed. They documented what they'd built. They wrote operational guides — not theoretical frameworks, but step-by-step accounts of how a distribution hub works, how to triage incoming donations, how to coordinate volunteer shifts when volunteers outnumber your ability to organize them. They trained other communities using those guides. Sandy Nurse, an OWS veteran who had worked with Occupy Sandy relief efforts in Midland Beach, went on to win a seat on the New York City Council. Devin Balkind, who had run tech and communication channels for both Occupy Wall Street and Occupy Sandy, launched Mutual Aid NYC during the COVID-19 pandemic in 2020, building a digital infrastructure for neighborhood-level relief across the city. And the broader network of people who had practiced disaster mutual aid during Sandy became the seed for Mutual Aid Disaster Relief — a national network whose steering committee includes veterans of both Occupy Sandy and the earlier Common Ground relief effort after Hurricane Katrina, explicitly designed around the principle that communities train their own disaster response capacity rather than waiting for institutional rescue.

The reproduction happened because the knowledge was documented and taught by people who'd done it. Not studied it. Done it. The credibility of the teaching came from visible struggle — Occupy Sandy's organizers could say "here's where our supply chain broke down on day three" alongside "here's how we fixed it by day five" because both were true and recent. The documentation wasn't polished. It didn't need to be. It needed to be honest about what worked, what failed, and what they'd do differently — the same three things your network knows from experience.

March for Our Lives, by contrast, survived by formalizing. After the Parkland shooting in February 2018, student organizers built three formal entities — a movement organization, an action fund, and a foundation. The

structure enabled persistence. March for Our Lives still operates. But the formalization required institutional overhead — legal counsel, board governance, fundraising infrastructure, nonprofit compliance — that most informal networks don't have access to and don't need.

The lesson isn't that formalization is wrong. It's that reproduction doesn't require it. What reproduction requires is documentation and teaching. Occupy Sandy's model spread because people wrote down what they learned and showed others how to do it. The starter kit your network produces in this chapter is the same act — the minimum viable mechanism for transmitting what you've built to someone who needs it.

In *The Matrix*, Neo's final act isn't a battle. It's a message. "I'm going to show these people a world you don't want them to see." The promise isn't victory. It's visibility — the act of revealing what's possible to people who didn't know it existed.

The network's starter kit operates on the same principle. You're not building a franchise or a manual for replication. You're documenting what you've seen become possible — that ordinary people in a specific place can build the skills, the trust, the coordination, and the civic infrastructure that the narrow path requires. The documentation is the message. The experience behind it is the proof.

This is where these pages can be transparent about something they've mostly left implicit.

The Narrow Path is a curriculum. It was designed to produce what your network has built — individual security practices, trusted relationships, a functioning group, inter-group coordination, civic infrastructure, shared principles. It used a fictional frame to make the learning engaging and the skills sticky. A researcher who encountered something at work that crystallized what she'd been feeling — and then did what researchers do. She went and found out how. She wrote it down, chapter by chapter, under a name that isn't hers, on a laptop she bought with cash.

The fiction served a purpose. It created urgency without manufacturing crisis. It provided a narrative arc that made thirty-six chapters of skill-building feel like a journey rather than a syllabus. It gave the curriculum a voice — mine — that could be personal without being prescriptive. And it kept the epistemological commitment intact: everything I cited is verifiable. The surveillance infrastructure is documented. The legal frameworks

are published law. The case studies are drawn from court records, journalism, organizational histories, and published research. The fiction was the frame. The content was always fact.

But your network's starter kit doesn't need the frame. Your authority doesn't come from a researcher's interpretation of documented patterns. It comes from practice. You've done the work in a real place, with real people, navigating real friction. When you write about what worked and what didn't, you're not translating someone else's findings. You're documenting your own.

That's why the network's version will be more honest than the curriculum that produced it. Not because the curriculum was dishonest — every claim in these chapters traces to documented reality, and that commitment doesn't change. But because the curriculum was designed for everyone, and the starter kit is designed for someone. Your community. Your terrain. Your specific challenges. The ground under your version is more solid because it's ground you've actually walked.

The starter kit is organized around four questions. These aren't prescriptive — adapt the structure to what your network needs. But they've worked in other contexts, and they cover the essential territory.

What are the essential skills?

Not everything from the full curriculum — the 80/20. If someone had one week to prepare, what would you prioritize? Your network has been through three levels of skill-building. You know, from experience, which skills changed how you operate daily and which were good to know but not essential in the first month. The threat model? Probably essential. The specific details of data broker opt-outs? Important, but can wait. Signal setup? Day one. The full history of COINTELPRO? Valuable context, but not the first week's priority.

The exercise of choosing forces a conversation about what matters most. That conversation is itself part of the learning.

What are the protocols that worked?

Your first-meeting script. Your security floor. Your decision-making process. Your facilitator rotation. Your debrief format. Your first joint action template. Some of these came from these pages. Some you invented. Some you adapted so significantly from the original that they're functionally yours. Write down the versions you actually use, not the versions the book provided. Include the modifications and why you made them — the

adaptations are the most valuable part.

What did you learn the hard way?

This is the honest section, and it's the most important one. What almost broke the group? What surprised you? What does no curriculum prepare you for? The groan zone when consensus stalled and someone almost walked. The security incident that wasn't an attack but felt like one. The joint action where coordination broke down and the debrief was harder than the failure. The institutional meeting that went differently than expected.

Write this section in specific terms, not abstractions. "Building trust takes longer than you expect" is true but useless. "We met every week for two months before anyone shared something personal, and the breakthrough happened over a mutual aid delivery, not a structured exercise" is something a new group can actually learn from.

What would you tell someone just starting?

In your own voice.

This is the section that no curriculum, no book, no researcher can produce. It's the part that comes from sitting in a room with people you've learned to trust, having done something together that none of you could have done alone, knowing that the capability you've built is real because you've tested it.

Write what you wish someone had told you. Write what you're glad no one told you because discovering it was the lesson. Write what you know now that you didn't know when you first checked your location history alone in your apartment, seeing for the first time how visible you were.

This question will produce the most disagreement and the best writing. Let it. The person who wants to say "it's worth it" and the person who wants to say "it's harder than anyone admits" are both telling the truth. Include both. A starter kit that only contains encouragement is useless. A starter kit that only contains warnings is discouraging. The honest version includes the weight and the reason for carrying it.

The starter kit is a real document. This isn't a reflection exercise.

When it's complete, share it through the liaison channel with every group in the network. Discuss it at a joint meeting. Revise it based on input from groups whose experience was different from yours. The revision process matters — it surfaces the assumptions each group made about what's essential, and the disagreements produce a better document than

any single perspective could.

If your network has identified groups or individuals who might be starting their own journey — people you've noticed at community meetings, neighbors who've asked questions, connections from institutional relationships — the starter kit is something you can share with them. Not as recruitment. As an offer. The same way this book was offered to you: here's what we learned, here's what we built, here's where we got it wrong. Take what's useful. Adapt it. Make it yours.

The act of producing the starter kit is itself the learning. It forces the network to synthesize months of experience into a coherent account of what mattered. It surfaces disagreements about priorities — disagreements that clarify the network's values as much as the shared principles document did. And it creates something that exists outside the book, outside the curriculum, outside the fictional frame. Something that belongs entirely to the people who built it.

Challenge

Produce the network's starter kit. This is a multi-meeting project — don't rush it.

Meeting 1: Draft. At a joint meeting, work through the four questions above. Assign each question to a small drafting team of two or three people drawn from different groups in the network. Each team produces a rough draft of their section before the next meeting.

Meeting 2: Assemble and revise. Bring the four sections together. Read them aloud. Discuss what's missing, what's redundant, what needs more specificity. The read-aloud is important — writing that sounds right on paper and writing that sounds right spoken to a real person are different, and the starter kit should sound like people talking, not like a document.

Meeting 3: Finalize and share. Incorporate revisions. Produce a version the network agrees represents its experience honestly. Share it through the liaison channel. Discuss: who should receive this beyond the network?

The starter kit should be short. One document. If it's longer than what someone would read in a single sitting, it's too long. The constraint is a feature — it forces the network to decide what actually matters versus what's nice to include.

Field Journal

Document the starter kit production process, not just the product. Which questions generated the most discussion? Where did groups disagree about what's essential? What did the revision process surface about the network's different experiences?

And note what it felt like to write the "what would you tell someone just starting" section. The distance between where you are now and where you started is the argument for everything the network has built. If the distance feels real when you write it down, the starter kit is working.

The curriculum was designed to produce you. You were designed to outgrow it.

Summary

Reproduction is the final act of learning. The network's most important product isn't a joint action or a monitoring report — it's the starter kit that transmits what you've built to the people who come after you. Near-peer teaching works because recent struggle creates better teachers than distant expertise. The starter kit documents your specific experience in your specific place, which is more useful than any general curriculum.

Action Items

- Produce the network's starter kit using the four-question framework: essential skills, protocols that worked, lessons learned the hard way, what you'd tell someone starting
- Assign each question to a drafting team of 2–3 people from different groups
- Read drafts aloud at a joint meeting — revise for honesty, specificity, and spoken voice
- Finalize and share through the liaison channel
- Identify potential recipients beyond the network — people you've noticed in community spaces who might be starting their own journey

Case Studies & Citations

- **Alcoholics Anonymous, Twelfth Step.** "Having had a spiritual awakening as the result of these steps, we tried to carry this message to alcoholics, and to practice these principles in all our affairs." The reproduction-as-completion principle: the program isn't finished until you've helped someone else begin. Standard AA literature.
- **Highlander Folk School / Highlander Research and Education Center.** Founded 1932 by Myles Horton in Monteagle, Tennessee. Popular education model: the answers to a community's problems exist within the community. Created conditions for communities to surface their own expertise rather than importing it.

Tennessee revoked its charter in 1961 in retaliation for civil rights activities; reincorporated as Highlander Research and Education Center.

- **Septima Clark and the Citizenship Schools.** Originally developed by Septima Clark, Esau Jenkins, and Bernice Robinson on Johns Island, South Carolina, beginning in the mid-1950s. Program transferred to SCLC in 1961. Clark, who had been fired from her teaching position in Charleston for NAACP membership, oversaw the establishment of roughly a thousand Citizenship Schools across the Deep South by the time she retired in 1970. Estimated ten thousand grassroots leaders trained. King called her "the Mother of the Movement." Sources: SNCC Digital Gateway; America Comes Alive; Highlander Research and Education Center Records.
- **Near-peer teaching and the protégé effect.** Research on peer tutoring shows that "teacher-slightly-ahead" models produce better outcomes for both teacher and learner than same-level collaboration or expert-to-novice instruction. The "protégé effect" describes the phenomenon where teaching deepens the teacher's own understanding. Sources: peer tutoring meta-analyses across educational psychology.
- **Occupy Sandy (2012).** OWS veterans mobilized roughly sixty thousand volunteers and over a million dollars in donations and supplies after Hurricane Sandy. DHS commissioned a study on their effectiveness. Veterans documented operational procedures and trained other communities. Key figures: Sandy Nurse (later NYC Council member, District 37); Devin Balkind (later founded Mutual Aid NYC in 2020); Michael Premo (co-founder of Occupy Sandy). Sources: THE CITY, October 2022; CBS New York, October 2022; DHS-sponsored report, "The Resilient Social Network," 2013; Mutual Aid Disaster Relief network.
- **Mutual Aid Disaster Relief (MADR).** National network growing from seeds of Common Ground (post-Katrina), Occupy Sandy, and other autonomous mutual aid efforts. Steering committee includes veterans of both. Explicitly designed around community-driven disaster response and the principle that communities train their own capacity. Sources: mutualaiddisasterrelief.org.
- **March for Our Lives (2018–present).** Student organizers after the Parkland shooting (February 14, 2018) built three formal entities: a movement organization, an action fund, and a foundation. Institutional formalization enabled persistence but required substantial overhead (legal, governance, fundraising, compliance). Contrasts with the documentation-and-teaching model of informal reproduction.

Templates, Tools & Artifacts

- **Starter kit four-question framework.** (1) What are the essential skills? (2) What are the protocols that worked? (3) What did you learn the hard way? (4) What would you tell someone just starting? Designed for multi-meeting production with cross-group drafting teams.
- **Starter kit production timeline.** Meeting 1: draft (assign questions to teams). Meeting 2: assemble, read aloud, revise. Meeting 3: finalize, share via liaison channel, identify recipients.

Key Terms

- **Near-peer teaching** — An educational approach where the teacher is only slightly more experienced than the learner. Works because proximity to the difficulty produces better instruction than distant expertise.
- **Protégé effect** — The phenomenon where the act of teaching deepens the teacher's own understanding of the material. Teaching forces you to organize and articulate knowledge in ways that learning alone doesn't require.

- **Reproduction** — In organizing, the process by which a group or network transmits its practices, knowledge, and experience to others who are starting. Distinguished from recruitment (adding members) and formalization (creating institutional structures). Reproduction requires documentation and teaching; it doesn't require institutional overhead.
- **Starter kit** — A short document produced by the network that captures essential skills, working protocols, hard-won lessons, and advice for people beginning the same work. Designed for a specific community and terrain, not as a general guide.

Chapter 36

The Path Is People

Look at what you've built.

Not the documents — the coalition agreements, the shared principles, the starter kit. Those matter, and you'll use them. But before you open any of them, look at the thing that no document contains.

You have people. Specific people in a specific place who know how to find each other, make decisions together, disagree without fracturing, and act when the situation requires it. You have groups that formed around kitchen tables and survived the groan zone. You have inter-group trust that was built through months of showing up — first as boundary-spanners, then as liaisons, then as a network that coordinates across the distance between you. You have civic infrastructure — monitoring relationships, institutional contacts, FOIA processes, shared channels — that didn't exist six months ago. You have a starter kit written in your own voice, tested against your own experience, ready to hand to someone standing where you stood at the beginning of this.

Sit with that for a moment. Give it the recognition it deserves.

The Montgomery Bus Boycott appears twice before this chapter. In Chapter 17: the MIA's transportation committee, the 300 cars, the 100 pickup stations, the operational infrastructure that sustained 381 days of coordinated action. In Chapter 26: the Women's Political Council's five years of preparation, Jo Ann Robinson printing 52,500 flyers overnight, readiness as the threshold — not courage, but preparation meeting its moment.

This chapter is about what happened after Montgomery won.

The boycott ended on December 20, 1956, when Montgomery's buses were desegregated by federal court order. That could have been the end. A local victory. An extraordinary one — but local. A city's buses, integrated. The infrastructure that sustained the campaign could have dissolved, the MIA could have returned to routine church business, and the model of

nonviolent mass action could have remained a single data point in a single Southern city.

That isn't what happened.

Within weeks of the boycott's end, Bayard Rustin — who had advised King during the boycott and who understood better than almost anyone how to translate a local victory into a regional capacity — drafted a series of working papers on expanding the Montgomery model. On January 10, 1957, approximately sixty Black ministers and civic leaders gathered at Ebenezer Baptist Church in Atlanta. The question they faced is the question your network faces now: we built something that works in one place. How does it spread?

The organization they formed — the Southern Christian Leadership Conference — was designed not as a membership organization but as a network of affiliates. Local churches, community organizations, groups already doing the work in their own cities. The SCLC didn't recruit individuals. It coordinated with existing local movements, providing what those movements couldn't generate alone: shared strategy, leadership training, and the institutional framework to sustain campaigns across state lines. Ella Baker, its first staff member and the person most responsible for its organizational DNA, insisted on developing local leadership rather than depending on charismatic figures. Septima Clark, who had been fired from her teaching position in Charleston for refusing to deny her NAACP membership, brought to SCLC the Citizenship Schools she had developed at the Highlander Folk School — about a thousand of them across the rural South by the time she retired. They trained local people to teach literacy and voter registration in their own communities. Near-peer teaching. The teacher who recently struggled with the material.

The model spread. Not because someone directed it from Atlanta, but because the pattern was visible and reproducible. In February 1960, four students at North Carolina A&T walked into a Woolworth's in Greensboro and sat at the whites-only lunch counter. They had the Montgomery boycott in their recent memory. They had the nonviolent method in their understanding. Within weeks, students in more than sixty cities were conducting sit-ins of their own. The Student Nonviolent Coordinating Committee formed that spring — not as a chapter of the SCLC but as an independent organization, drawing on the same principles, adapting them to a younger generation's tactics and a different form of direct action. SNCC's organizers stressed developing self-reliant local leaders to sustain grass-

roots movements. The model reproduced. It mutated. It became something its originators hadn't planned and couldn't control.

The Freedom Rides of 1961 followed. An interracial group organized by the Congress of Racial Equality rode interstate buses through the South to test federal desegregation rulings that Southern states had ignored. When CORE's original riders were beaten and firebombed in Alabama and CORE considered ending the campaign, Diane Nash and SNCC's Nashville activists organized new riders to continue. CORE, SNCC, and SCLC formed a Freedom Riders Coordinating Committee. Over the summer of 1961, more than sixty Freedom Rides crisscrossed the South. The organizations coordinated without merging. They maintained separate identities, separate decision-making structures, and separate tactical approaches while acting in concert toward a shared objective.

The 300 cars and 100 pickup stations in Montgomery were infrastructure for something larger than Montgomery. The WPC's five years of preparation, the MIA's operational logistics, the mass meetings at rotating churches — all of it was practice for a capacity that hadn't fully revealed its purpose yet. The boycott's victory wasn't the endpoint. It was the proof of concept for a network that, over the next decade, changed the legal and social structure of the country.

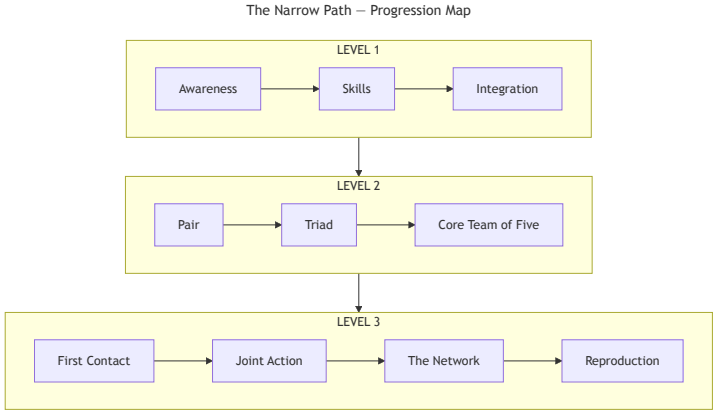
The parallel is not that your network will do what the civil rights movement did. The parallel is structural. You built something in a specific place. You proved it works. The starter kit you produced is your version of the working papers Rustin drafted after Montgomery — documentation of a model, written by people who did it, available to others who need it. What happens next depends on who finds it, what they build, and whether the preparation meets its moment.

In *The Hunger Games*, the end of the games was the beginning of the story. The districts had been kept separate by design — isolated, unable to see each other's strength, unable to coordinate. The system worked as long as the separation held. When the districts found each other, the architecture of control couldn't function the way it was built to. The final image of the story isn't a battle. It's a country rebuilding — slowly, imperfectly, without a script.

This book was organized as a path. Chapter by chapter, level by level, building from individual awareness through group formation through net-

work coordination to reproduction. You read it in sequence because the skills built on each other. The first-contact protocol assumed nothing about inter-group trust. The governance frameworks assumed you'd completed joint actions. The shared principles conversation assumed you'd weathered inter-group conflict. The sequence was the pedagogy.

You don't need the sequence anymore.



From here, the book is a reference shelf. You pull what you need when you need it. A new group approaches your network and you need the first-contact protocol — that's Chapter 27. A governance question surfaces that the existing coalition agreement doesn't cover — Chapter 30's decision domain mapping. Two groups are in conflict and the liaisons can't resolve it — Chapter 32's mediation process. The network is growing and a new group needs onboarding — Chapter 34's probationary coordination protocol. Someone asks you how to start — you hand them the starter kit, and if they want the longer version, you point them to the earlier chapters.

Organized by what you might need:

Recognizing and vetting another group: Chapter 27 — behavioral recognition, boundary-spanner protocol, Zaheer's inter-organizational trust framework.

Establishing shared security across groups: Chapter 28 — inter-group information-sharing agreement, compartmentalization as care, liaison communication model.

Planning and debriefing joint actions: Chapter 29 — first joint action design, the debrief-as-learning framework, complementary action model.

Governance and decision-making: Chapter 30 — consent-based governance,

decision domain mapping, spokes council structure, coalition agreement template.

Navigating institutions and geographic difference: Chapter 31 — co-optation dynamics, complementary partnership model, rural coordination adaptations.

Handling inter-group conflict and sustaining the network: Chapter 32 — three-step escalation protocol, network health check, rotating roles.

Civic monitoring and shared infrastructure: Chapter 33 — Observer Corps model, FOIA as civic tool, network-level civic infrastructure.

Shared principles and structural accountability: Chapter 34 — Freeman's structurelessness diagnostic, shared principles process, onboarding protocol.

Producing materials for others: Chapter 35 — near-peer teaching, starter kit framework, reproduction as completion.

The first twenty-six chapters cover individual skills and group formation — threat modeling, password security, metadata awareness, social engineering defenses, secure communication, information verification, the social adoption problem, trust building, facilitation, conflict resolution, collective action, and the case for finding others. Those chapters remain independently useful. A new person joining the network can work through them at their own pace. The skills don't expire.

Challenge

This challenge mirrors the first one in Chapter 1. That chapter asked you to open your location history and look at it. To see how visible you were. To sit with that.

This chapter asks you to look at what you've built. The people, the practices, the infrastructure, the connections. Not the documents — the capacity. What your network can do today that no individual in it could have done alone six months ago.

Sit with it.

Then write down what you would tell the person you were at the beginning — before the threat model, before the group, before any of it. Not advice, exactly. What you know now that you didn't know then. What you'd want that person to hear.

Write it for whoever comes next. Not for the book. Not for the network's records. For the person who hasn't started yet and might need to hear it from someone who has.

Field Journal

The field journal began as a personal record — notes to yourself about what you noticed, what you tried, what changed. It became a shared group reference. Then a network coordination tool. Coalition agreements, debrief findings, civic monitoring observations, shared principles.

This is its last prescribed entry. After this, the field journal is whatever the network needs it to be.

Record what the network looks like today. Not an assessment — a snapshot. How many groups. What you're working on. What's functioning and what's still unresolved. What you're worried about. What you're proud of. Date it. You'll want this record later, the same way you wanted the record of your first threat model later — not because it tells you something you've forgotten, but because the distance between then and now is the clearest measure of what you've built.

I started writing these chapters alone in my apartment, on a laptop I bought with cash, publishing under a name that isn't mine, trying to turn what I'd seen during that evaluation session into something other people could use. I didn't know if anyone would find them. I didn't know if the skills I'd researched would hold up in practice, in communities I'd never visited, facing challenges I could only study from a distance. I didn't know if the path I'd found in the research was real or an artifact of a researcher who wanted too badly to find hope in the data.

I still don't know all of that. The path was always narrow, always contingent, always dependent on people doing specific things in a specific window.

What I can tell you is what the documented record shows. The skills work. The organizing traditions I drew from — the ones I translated into these chapters — have been tested across decades and contexts. The case studies are real. The infrastructure you've built is real. The network functions because you built it to function, maintained it through friction, and

adapted it when the protocols didn't fit your terrain.

The curriculum is complete. The tools are in your hands.

A society grows great when old men plant trees in whose shade they shall never sit.

Summary

This is the final chapter. The network's journey from first contact through joint action through shared principles to reproduction is complete.

Action Items

- Look at what the network has built — people, practices, infrastructure, connections — and sit with it
- Write what you would tell the person you were at the beginning
- Write it for whoever comes next
- Record a snapshot of the network as it exists today: groups, projects, functioning systems, unresolved challenges
- Date the snapshot — this becomes the baseline for measuring future growth
- Use the reference library index above when specific needs arise

Case Studies & Citations

- **Montgomery Bus Boycott — reproduction.** Boycott ended December 20, 1956 (federal court order). Bayard Rustin drafted working papers on expanding the Montgomery model. January 10, 1957: approximately sixty Black ministers and civic leaders met at Ebenezer Baptist Church, Atlanta. Organization formed: Southern Christian Leadership Conference. Sources: King Institute, Stanford University; BlackPast.org; National Park Service; SCLC Wikipedia article citing *Papers of Martin Luther King Jr.*, Vol. 4.
- **SCLC as network of affiliates.** Designed as a coordinating body for existing local movements, not as an individual membership organization. Provided shared strategy, leadership training, and institutional framework across state lines. Contrasts with NAACP (individual membership, local chapters) and CORE (similar). Ella Baker: first staff member, insisted on developing local leadership over charismatic dependency. Sources: King Institute; crmvet.org Civil Rights Movement history.
- **Septima Clark and the Citizenship Schools.** Originally developed by Clark, Esau Jenkins, and Bernice Robinson on Johns Island, South Carolina, mid-1950s, under the Highlander Folk School. Program transferred to SCLC in 1961. Clark oversaw roughly a thousand schools across the Deep South by her 1970 retirement, training an estimated ten thousand grassroots leaders. King called her "the Mother of the Movement." Sources: SNCC Digital Gateway; America Comes Alive; Highlander Research and Education Center Records; Clark, *Echo In My Soul* (1962).
- **Greensboro sit-ins (February 1960).** Four students at North Carolina A&T — Ezell Blair Jr. (Jibreel Khazan), David Richmond, Franklin McCain, and Joseph McNeil — sat at a Woolworth's whites-only lunch counter. Within weeks, students

in more than sixty cities conducted sit-ins. Led directly to SNCC's formation that spring.
- **Student Nonviolent Coordinating Committee (SNCC).** Founded April 1960 at Shaw University, Raleigh, North Carolina, at a conference organized by Ella Baker. Independent organization, not a chapter of SCLC. Stressed developing self-reliant local leaders. Sources: SNCC Digital Gateway; Zinn, *SNCC: The New Abolitionists* (1964).
- **Freedom Rides (1961).** Organized by Congress of Racial Equality (CORE) to test federal desegregation rulings. After original riders beaten and firebombed in Alabama, Diane Nash and SNCC Nashville activists organized new riders. CORE, SNCC, and SCLC formed a Freedom Riders Coordinating Committee. More than sixty rides over the summer of 1961. Organizations coordinated without merging — maintained separate identities and decision-making while acting in concert.

Templates, Tools & Artifacts

- **Reference library index.** (Above.) Organized by function — maps each coordination need to the specific chapter and tools that address it. Designed for non-sequential consultation after completing the curriculum.
- **Final field journal prompt.** Snapshot: how many groups, what you're working on, what's functioning, what's unresolved, what you're worried about, what you're proud of. Date it.
- **"What would you tell someone starting" prompt.** Write for the person who hasn't begun yet. Not advice — what you know now that you didn't know then.

Key Terms

- **Network of affiliates** — An organizational model where existing local groups coordinate through a shared framework without merging into a single organization. Each affiliate maintains its own identity, leadership, and decision-making. The SCLC model: coordination without centralization.
- **Reproduction** — The process by which a network transmits its practices and knowledge to others. Distinguished from growth (adding members or groups) and formalization (creating institutional structures). Reproduction requires documentation and teaching; the starter kit is the minimum viable mechanism.
- **Reference library** — The mode this book enters after completion. No longer read sequentially; consulted by function when specific needs arise. The shift from curriculum to reference library is the structural marker of the network's independence from the material.