HOW TO MOVE PEOPLE

An instructional guide to human movement operations under hostile conditions

Synthesized from: LiNK rescue operations · Afghan evacuation networks 2021 · SOE tradecraft · Danish resistance 1943 · EFF Surveillance Self-Defense · PEN America · contemporary humanitarian corridor doctrine

---

This guide is instructional, not theoretical. It synthesizes what has actually worked — and what has failed — across the most studied contemporary and historical human movement operations: Liberty in North Korea's 3,000-mile rescue route; the improvised Afghan evacuation networks of August 2021; the Danish rescue of October 1943; British SOE clandestine network doctrine; and current digital security practice as documented by the EFF, PEN America, and activist security trainers.

The organizing insight across all these cases is this: networks that moved people successfully rarely failed at the movement phase. They failed at the legal destination problem, the financing problem, the broker reliability problem, or the communication security problem. This guide addresses all four, in the order you will encounter them.

> **READ FIRST** Before building anything, read Section 1 in full. Every mistake documented in these cases traces back to skipping threat modeling and jumping to logistics.

SECTION 1

Before You Build Anything: Threat Modeling

Threat modeling is not paranoia management. It is the discipline that determines whether every subsequent decision — what routes to use, how to communicate, who to trust, where to hide people — is calibrated to your actual situation or to a fantasy version of it.

Every documented network failure can be traced to a threat model that was wrong in one of three directions: it underestimated the adversary's reach (the French Resistance's Prosper network, rolled up because organizers assumed the Gestapo couldn't penetrate that far); it overestimated the adversary's coherence (the Danish rescuers nearly quit when they assumed German patrols were coordinating, when in fact Wehrmacht units were looking the other way); or it had no threat model at all and was improvising reactively (early Afghan vet networks in August 2021 that created legal limbo for thousands by moving people without a receiving plan).

The Four Questions

Answer these before anything else. Write nothing down. Commit the answers to memory, share them only in the smallest necessary group.

1. WHO is the specific adversary? Not 'the government' — which agency, which unit, which jurisdiction? A municipal police force with no federal coordination is a fundamentally different adversary than a federal intelligence apparatus with signals capacity. The North Korea network's primary adversary in the China leg is the Chinese Ministry of Public Security, not the North Korean regime — knowing this determines everything about how the China leg operates.
2. WHAT do they want? Are they trying to prevent movement, identify the network, or make an example? These require different responses. An adversary trying to stop movement can be evaded. An adversary trying to map the network means your counter-measure is compartmentalization, not speed.
3. HOW do they actually operate? Surveillance capability, checkpoint patterns, patrol timing, informant networks, legal authority to enter specific spaces. The Danish rescuers knew that German authorities needed a political justification to enter Danish hospitals — so hospitals became staging points. You need the equivalent local knowledge for your specific terrain.
4. WHEN does their attention increase? Specific days, events, political moments, shifts in command, budget cycles? The Afghan network in August 2021 had a closing window that was visible — the airport was the only safe exit and everyone knew the deadline. The North Korea network after COVID faced a fundamentally different adversary tempo than before — patrol intensity jumped, bribe rates doubled, and routes that worked in 2019 stopped working in 2022.

Calibrating Your Model to Reality

Two common errors in threat modeling:

— Flattery bias: treating the adversary as more sophisticated than they are, which leads to operational paralysis. The Danish rescue worked partly because the rescuers correctly assessed that the Gestapo's capacity in Denmark was thin and their political will was constrained. An accurate threat model enabled boldness.

— Flattery bias in reverse: treating the adversary as less sophisticated than they are because you want them to be. The French Resistance's catastrophic network losses in 1943-44 came from organizers who knew the Gestapo was good but assumed their specific circuit was clean. Assume nothing is clean that you haven't actively verified.

LESSON	The correct threat model is not the most terrifying one. It is the most accurate one. Reassess your threat model whenever: someone is arrested, a route is compromised, the political situation shifts, or you are expanding the network.

Network Architecture: How to Structure the Operation

Every successful human movement operation — from the 1943 Danish rescue to Liberty in North Korea's current routes — uses the same underlying structure, arrived at independently. The structure is not doctrine for its own sake. It is what survives compromise.

The Cell

A cell is three to seven people who know each other and collaborate directly on a single defined function. The cell is the basic unit of the network. Its boundaries are not bureaucratic — they are the network's immune system.

What a cell knows:

- The identities and roles of its own members
- A single point of contact outside the cell — not a name, ideally, but a contact method
- Its own function and the handoff point where its function ends and the next begins

What a cell must not know:

- The identity of other cells
- The full route — only the segment it operates
- Leadership structure above its immediate contact
- Anything about financing that it doesn't need to operate its specific function

> **CRITICAL** Liberty in North Korea explicitly does not reveal the identities of its brokers and guides in China and Southeast Asia even in public communications about the route. This is not evasiveness — it is cell discipline. The moment a name is attached to a function, that name becomes a target.

The Phases of Movement and Why They Must Be Separate

The Danish rescue is the cleanest historical example of phase separation. Different cells handled different phases with deliberate handoff points between them:

PHASE 1	Warning and initial concealment Who is at risk, where are they now, where can they go in the next 12 hours

PHASE 2	Moving people to the transit point

	From hiding locations to the coast — short-haul movement, high local knowledge requirement

PHASE 3	The transit itself The fishermen — specialized skill, specific equipment, specific timing knowledge

PHASE 4	Reception at the destination The Swedish side — a completely separate network that the Danish side had minimal direct contact with

Liberty in North Korea's route has the same structure: brokers handle the China-to-Southeast Asia leg; LiNK field staff meet refugees only at the end; receiving networks in South Korea and the US are entirely separate organizations. No single person knows the full route. No compromise at one phase can cascade to the others.

The Afghan evacuation networks of 2021 failed this principle under pressure. Because the window was closing in hours rather than days, networks that had not pre-built phase separation improvised connections — and created legal limbo for thousands of people who were moved without a functioning reception phase on the other side.

> **LESSON** Phase separation is not a luxury for when you have time to plan. It is the minimum viable architecture. Build it first, even if each phase initially has only one person in it.

The Liaison Function

The liaison carries information between cells without knowing the content or context of what they carry. This is a structural role, not a trusted insider role. The liaison is told only what they need to convey.

In the SOE model, messages that couldn't be committed to memory were written on tissue paper carried in cigarettes — able to be swallowed or destroyed instantly. The contemporary equivalent is: no written record at all, and anything communicated to a liaison is stated in terms that are operationally useful to the recipient but meaningless to anyone who intercepts the courier.

- Wrong: 'Tell them to move the family from the apartment on Tuesday.'
- Right: 'The bird is ready on the 14th.' — and only the recipient knows what 'bird' and '14th' mean in this context.

When and How to Expand the Network

Every successful large-scale operation — the Danish rescue scaling to 56,000 underground members by war's end; the Afghan alumni network spinning up in hours from a university listserv — expanded through pre-existing trusted social infrastructure rather than through outreach to strangers.

The Danish rescue worked because Danish Lutheran churches, medical institutions, and universities were already internally cohesive communities with existing trust relationships and shared values. The network didn't create trust — it activated trust that already existed and redirected it toward the operation.

> **RULE** Expand through people who already trust each other for reasons unrelated to the operation. Never recruit a stranger. Expansion through unknown contacts is the single most common cause of network penetration by informants.

SECTION 3

The Broker Layer: Local Knowledge You Cannot Replace

Every documented contemporary movement operation relies on local brokers or guides whose function is irreplaceable by any outside organization or general doctrine. The North Korea network's China leg runs on brokers. The Afghan network ran on local drivers, fixers, and border guides. The Danish fishermen were brokers who knew the specific patrol patterns of the specific German naval units in the specific waters they were crossing.

The broker layer is simultaneously the most operationally essential element of the network and the highest-risk element. Understanding why — and how to manage the tension — is one of the most important skills in this work.

What Brokers Know That You Cannot Know

- The specific timing and pattern of checkpoint operations in their area
- Which officials can be approached and under what circumstances
- Which routes have gone quiet and which have recently become active
- The community relationships that create cover for movement — who owns the vehicles, who runs the business, who has a reason to be in a place
- The current cost and risk calibration — what was safe last month may not be safe now

This knowledge is not writable. It is accumulated through presence, relationship, and continuous observation. Liberty in North Korea has operated for over two decades and still relies on local brokers in China and Southeast Asia rather than deploying its own field staff into the high-risk

early legs of the route. This is not a temporary gap — it is a structural acknowledgment that local knowledge cannot be imported.

Managing Broker Reliability

Brokers are not members of your network. They are contractors, often motivated primarily by payment. This is not a moral judgment — it is an operational fact that determines how you work with them.

1. Never give a broker more information than the specific task requires. A broker who moves people from Point A to Point B does not need to know why, where they came from, where they are going after, or anything about the broader network.
2. Do not use a single broker as a single point of failure. Where possible, build redundant broker relationships on each leg. When LiNK's costs spiked after COVID, networks with redundant broker relationships had options; those with single-broker dependency were paralyzed.
3. Pre-establish clear payment terms and document nothing. Payment disputes create pressure that can lead to disclosure. If the terms are not agreed in advance, the broker has leverage over you at the worst possible moment.
4. Know the difference between a broker who has gone quiet because they are busy and a broker who has gone quiet because they have been compromised or arrested. Pre-establish a dead-man protocol: if no contact within X hours after a scheduled handoff, assume the worst and activate the fallback.

The Informant Risk

In China, North Korean defectors are vulnerable to being turned over by brokers who fear or have been pressured by authorities. In Afghanistan in 2021, some Taliban-era informants were embedded in civilian populations that networks trusted. In every hostile environment, the adversary attempts to penetrate the broker layer because it is the most accessible entry point into the network.

There is no reliable way to vet a broker against informant risk. The mitigation is structural: because brokers know only their specific segment, a compromised broker can only expose that segment. The cell structure is the defense. It does not prevent infiltration — it limits the damage when infiltration occurs.

Communications Security: How to Talk Without Being Heard

The adversary landscape for communications has changed more radically in the past decade than any other aspect of this work. Authoritarian governments — Russia, China, Myanmar, Iran, North Korea — have developed or purchased sophisticated interception, surveillance, and metadata analysis capacity. Global internet freedom declined for the fifteenth consecutive year in 2025. Russia blocked Signal in 2024. Myanmar criminalized anticensorship tools in 2025.

This does not mean secure communication is impossible. It means you must understand what each communication method protects and what it does not.

The Channel Hierarchy: Safest to Least Safe

TIER 1: IN PERSON	The most secure channel when correctly executed. Requirements: location has no listening devices, no surveillance of the approach, and the meeting does not create a visible pattern. North Korean defectors communicate with family inside North Korea from mountains at night — they move to a different location each time to avoid creating a pattern that surveillance can map. A meeting that happens at the same café, same time, every week is not secure in-person communication. It is a schedule.

TIER 2: END-TO-END ENCRYPTED MESSAGE	Signal is the current standard. It protects message content. It does not protect metadata: who is communicating with whom, when, how often, and from where. Delete messages immediately after reading. Use disappearing messages set to the shortest interval the operation can sustain. LiNK provides refugees with a dedicated rescue phone — a device not associated with their personal identity — for communication during the route. This is the correct model: operational communications happen on devices with no personal history.

TIER 3: CODED PUBLIC SIGNAL	The British used BBC French Service broadcasts — innocuous phrases that meant operational things only to the intended recipient. The contemporary equivalent: a social media post, a hashtag pattern, a specific image published at a specific time — carrying meaning that is invisible to anyone who doesn't know the code. This channel is useful for broad signaling to a distributed network when direct contact creates risk. The code must be established in advance through a higher-tier channel. Never establish a code over the channel you intend to use it in.

TIER 4: WRITTEN MATERIAL	Lowest priority. Highest risk. Anything written is evidence. The SOE rule: anything that cannot be committed to memory is written on tissue paper, carried in a way that permits immediate destruction. The contemporary rule: nothing persists. No screenshots. No forwarded messages. No copied notes. If it must be written, it must be destroyable.

Metadata: The Problem You're Probably Not Solving

Most people in underground operations focus on message content — what is being said — and underinvest in metadata security — who is talking to whom, when, and from where. Metadata is often more dangerous than content because it reveals network structure without requiring the adversary to decrypt anything.

- A phone that is always present at the same location at the same time every Tuesday creates a pattern that surveillance can read even without accessing any messages.
- An account that is accessed exclusively from one IP address is effectively identified regardless of what username it uses.
- A communication pattern that shows three people contacting a fourth in rapid sequence after a specific event reveals organizational hierarchy more clearly than any message content.

Specific practices that address metadata rather than just content:

1. Operational devices must not be associated with personal identity. Not through the billing account, not through the email used to set it up, not through behavioral patterns (logging in from home, from work, on a regular schedule).
2. Power off — not silence, not airplane mode — personal mobile devices before sensitive meetings. Carrier networks track location continuously. This is not defeated by location services settings.
3. Access operational accounts from non-personal network connections. A coffee shop you visit once is better than your home network. The Tor browser adds another layer.
4. Disable biometric unlock before any encounter with authorities. In most jurisdictions, law enforcement can legally compel biometric unlock. They cannot legally compel passcode disclosure. This is not a minor distinction — it is the difference between your device being a liability and being neutral.

When Communication Goes Silent

Pre-establish a protocol for silence before you begin operations. In the SOE model: if a scheduled contact does not occur, the network has a defined window (24-48 hours was the

manual's recommendation) during which the absent member is buying time, and within which the network must assume potential compromise and act accordingly.

In contemporary operations: if a broker does not check in within the pre-agreed window after a handoff, the fallback contact is activated, the route is frozen, and no one moves until the situation is assessed. The worst outcomes in the North Korea network have come from networks that interpreted silence as busy rather than as compromised and continued to move people into a segment that was already being monitored.

SECTION 5

Moving People: The Route, the Staging, and the Handoff

This section covers the practical mechanics of moving a person or a group from a dangerous location to a safer one. The principles apply whether the transit takes hours or months, whether the distance is across a city or across three countries.

Route Design

A route is not a path. It is a system of paths, with a primary and at least two backups, selected based on adversary pattern analysis rather than convenience.

- The primary route is the one you use when conditions are normal.
- The first backup is the one you use when the primary is compromised but the timeline is still intact.
- The second backup is the one you use when both the primary and first backup are compromised — this route accepts higher risk in exchange for movement.
- The abort protocol is not a route. It is the answer to: if all routes fail, where does the person shelter and for how long, and who is responsible for their situation during that time.

Route selection principles drawn from documented operations:

- Narrow crossings first. The Danish routes concentrated on the narrowest points of the Øresund strait. Distance in hostile territory is not neutral — it is accumulated exposure. Minimize transit time in the most dangerous segments, even if it means longer preparation or staging time.
- Use institutional cover where available. Danish hospitals functioned as staging points because authorities needed political justification to enter them. What institutions in your terrain have equivalent protection — physical, legal, or reputational — that creates friction for adversary interference?

— Timing matters more than routing. A route through a checkpoint that operates only between 6am and 10pm is safer at midnight than any alternate route without checkpoints. Adversary temporal patterns are as important as adversary geographic patterns.

— Local knowledge drives all decisions. No route designed from outside the terrain by people without current local presence is reliable. The broker layer exists to provide this knowledge. Trust it over map-based reasoning.

Staging: The Safe Harbor

A safe harbor is any location where a person can wait between phases without exposure. It is not permanent. It is a node in the route.

Effective safe harbors:

— Appear unremarkable from outside — no unusual traffic, no visible change in pattern

— Have at least two exits that are known to the person sheltering there

— Are known to as few network members as possible — only the people who need to use it

— Have institutional cover (a clinic, a business, a religious institution) that explains occupancy and creates legal friction for adversary entry

— Are used for the shortest time operationally possible — the longer a location is used, the more it builds a pattern

The hard limit on safe harbor usage that the SOE manual makes explicit and that contemporary operations confirm: any location that develops a visible association with movement activity must be abandoned immediately. The moment a pattern is visible, the location is no longer safe — it is a trap.

The Handoff

The handoff is the highest-risk moment in any movement operation. It is where two cells that should not directly know each other must briefly interact. Every documented operational failure that occurred during movement rather than planning happened at or near a handoff.

1. Pre-establish recognition protocols that don't require names. A specific phrase, a physical signal, an object. The SOE model: passwords must be given word-perfect or they are not accepted. This is not pedantry — it is the security function of the protocol.
2. The handoff location should not be the same as the staging location. Moving from shelter to the handoff point is itself a transit. Treat it as one.
3. Minimize time at the handoff point. The handoff is not a meeting. It is a transfer. The less time spent in the transfer state — where both cells are briefly visible — the safer.
4. After handoff, the delivering cell has no further contact with the person and no knowledge of the next stage. This is not coldness. It is the structural protection that means a compromise on the receiving end cannot cascade back.

SECTION 6

The Legal Destination Problem: The Failure Point No One Plans For

This is the lesson that distinguishes the contemporary cases most sharply from the historical models, and it is the lesson that is most consistently ignored by networks that are good at movement but bad at outcomes.

The most well-documented failure mode of the Afghan evacuation networks of 2021 was not extraction — tens of thousands of people were successfully moved out of Afghanistan in August of that year. The failure was destination: people arrived in the UAE, in Pakistan, in other transit countries, and had no legal status and no clear path forward. Some remained in UAE holding camps for nearly two years. The networks had solved the movement problem and had not solved the legal status problem.

The North Korea network solves this by routing people through countries that will process them to South Korea, which has a legal framework for receiving North Korean defectors. The entire 3,000-mile route is designed around the destination's legal capacity, not just the transit path.

The Danish rescue solved this by securing Swedish agreement to accept refugees before the operation began at scale. Sweden was the legal destination. The fishermen were the transit mechanism. The legal destination came first.

Plan the Legal Destination Before the First Movement

The destination is not where the person arrives geographically. It is where the person has legal status — the ability to exist, to work, to access services, to not be returned to the place they fled.

- What legal status will the person hold at the destination? Refugee, asylum seeker, parole, visa, citizenship? Each carries different rights and different timelines.
- What is the processing path and realistic timeline? The Afghan SIV process had a 17,000-application backlog in August 2021. Any network operating at that time needed to have a plan for the gap between movement and status resolution.
- What does the destination country's relationship with the origin country look like? China's forced repatriation policy for North Korean defectors means no destination in China is a legal destination — it is only a transit point. A network that treats China as a destination rather than a transit leg is building toward repatriation.
- What is the reception capacity? A person who arrives at a legal destination with no receiving organization, no housing plan, no legal representation, and no language access is not safe — they are differently endangered.

Building the Receiving Infrastructure

The receiving side of the operation requires entirely different skills than the transit side — legal knowledge, resettlement support, language capacity, community connection. It also requires a different kind of organization: one that can operate openly, interface with government systems, and sustain relationships over years rather than weeks.

Liberty in North Korea maintains a Resettlement Assistance Program as a distinct arm of its work, explicitly separate from the rescue route operation. Afghan resettlement organizations — IRC, UNHCR, and dozens of smaller groups — constitute a receiving infrastructure that took decades to build. The Danish receiving infrastructure was Sweden itself: a functioning state with established institutions that could absorb refugees immediately.

> **RULE** If you do not have a legal destination plan before the first movement, you are moving people from one form of danger to another. Complete the destination infrastructure first. Movement without destination is not rescue.

SECTION 7

Financing: The Constraint That Determines Scale

Every operation documented in this synthesis ran into the money problem. The Danish rescue cost approximately 20 million kroner — about half paid by Jewish families, half by wealthy Danish donors. The class dynamic this created meant working-class families were priced out or paid rates that consumed their savings. Liberty in North Korea charges $3,000 per rescue and explicitly uses a free passage model — the refugee does not pay — funded by donor contributions. Before the pandemic, North Korean defection cost about $13,000 per person; after the COVID border crackdown, that figure reached $21,000.

The financing structure of an operation is not a logistics detail. It determines who can be moved, who gets left behind, and what leverage the broker layer has over the network.

Principles of Underground Finance

- **—** Cash only. No transaction records, no digital transfers that leave a trail, no financial identities that can be subpoenaed or frozen. The remittance networks serving North Korean defectors operate through three-party broker arrangements specifically to avoid any single traceable transaction.
- **—** No single large source. Concentrated funding creates concentration risk — a donor who stops giving, an account that is frozen, a network that is identified through unusual financial activity. Distributed small contributions are operationally more resilient than single large grants.

— Finance the network before you need it. The North Korea network's cost spike after COVID paralyzed operations that had not built financial reserves. A network that can only operate when current funding is flowing cannot absorb disruption.

— Separate finance from operations. The person who manages money should not know operational details. The person who runs the route should not handle money beyond immediate operational expenses. This is both security discipline and corruption prevention.

— Anticipate that costs will increase under pressure. Every documented case shows the same pattern: when adversary pressure increases, broker costs go up, bribe rates go up, and the financial model that worked under normal conditions fails. Build your financial reserves for the high-pressure scenario, not the baseline.

SECTION 8

When the Network Is Compromised: What to Do

Assume compromise will happen. Every network that operates long enough will experience it. The question is not whether your network will be penetrated or a member arrested — it is whether the structure you built allows the network to absorb that compromise and continue, or whether it cascades into collapse.

The Immediate Response to Known Compromise

1. Freeze all movement immediately. No one moves through the affected segment until the situation is assessed. This is non-negotiable. The worst outcomes documented — in the North Korea network, in the French Resistance — came from networks that continued to move people into segments they already knew were compromised.
2. Notify only the immediately necessary people. Compromise of a cell should not travel up the chain unless operationally necessary. The goal is containment. Broad notification creates broad exposure and enables panic decisions.
3. Activate backup contacts and backup routes. These must exist before the compromise, not be improvised after.
4. Give the compromised member time if they are in custody. The SOE's rule was 48 hours — enough time for the network to reorganize before any information extracted under duress could be acted on. Your network needs an equivalent window pre-established.
5. Assess what the adversary now knows. Map the compromised member's knowledge against the cell structure. If they knew only their segment, the damage is contained. If they knew more, that wider scope of knowledge must be treated as compromised and those segments frozen.

Legal Preparation Before It Is Needed

PEN America's guidance for at-risk communities converges with SOE doctrine on a point that feels administrative until the moment it is urgently necessary: legal support must be established before you need it, not after an arrest.

- Every member of the network should know, without looking it up, who to call immediately upon detention.
- Every member should know what not to say — which is almost everything beyond their name and a request for legal representation.
- Pre-establish relationships with legal organizations that handle political detention, immigration cases, and related matters in your jurisdiction.
- Know the specific legal rights in your specific jurisdiction. The legal landscape differs significantly: in some jurisdictions, biometric unlock can be compelled; in others, passcode disclosure cannot. In some, a warrant is required for digital search; in others it is not. Your members need to know the specific rules of the specific terrain they are operating in.

Operational Security as Culture, Not Checklist

The most durable finding across all these cases is that networks whose members had internalized operational security as habit — not as a protocol they consulted — survived longer and recovered from compromise more effectively.

The minimum footprint principle: carry nothing unnecessary, know nothing unnecessary, say nothing unnecessary. This is not a set of rules. It is a disposition. A member who has internalized it does not need to remember what not to do — they naturally default to the least-revealing option at every decision point.

Morale is an operational asset. The SOE training materials recognized that burned-out, isolated operators make mistakes. The Danish resistance grew from a small underground to tens of thousands partly because participants experienced successful collective action that reinforced the culture. Design the operation to have visible, achievable milestones — not just against eventual outcome, but against the daily reality of participating in something that matters and is working.

SUMMARY

The Eight Lessons

LESSON 1	Threat model before you build anything. An inaccurate adversary model will destroy an otherwise sound operation.

LESSON 2	Phase separation is the minimum viable architecture. No single person should know the full route. Build the cell structure first.

LESSON 3	The broker layer is irreplaceable. Local knowledge cannot be imported. Manage brokers structurally — they are contractors, not members.

LESSON 4	Metadata kills networks as often as message content does. Secure your communication patterns, not just your message text.

LESSON 5	Route design is adversary pattern analysis, not map reading. Timing, institutional cover, and local knowledge drive all decisions.

LESSON 6	Movement without a legal destination is not rescue. Solve the destination problem before the first person moves.

LESSON 7	Finance determines who gets moved and who gets left behind. Build financial reserves for high-pressure conditions, not baseline.

LESSON 8	Assume compromise will happen. The structure you build determines whether it is contained or catastrophic.

This document is a historical and educational synthesis. The principles described are drawn from publicly available scholarship, declassified documents, journalistic reporting, and civil liberties guidance.