How Corporations Work to Undermine Grassroots Resistance, and How to Stop Them

March 8, 2021 Deep Green Resistance News Service Leave a comment

In this article Max Wilbert outlines the political and environmental need for security culture. He offers recommendations to secure communications.

By Max Wilbert

For 50 days, the Protect Thacker Pass camp has stood here in the mountains of northern Nevada, on Northern Paiute territory, to defend the land against a strip mine. Lithium Americas, a Canadian corporation, means to blow up, bulldoze, or pave 5,700 acres of this wild, biodiverse land to extract lithium for "green" electric cars. In the process, they will suck up billions of gallons of water, import tons and tons of waste from oil refineries to be turned into sulfuric acid, burn 11,000 gallons of diesel fuel per day, toxify groundwater with arsenic, antimony, and uranium, harm wildlife from Golden eagles and Pronghorn antelope to Greater sage-grouse and the endemic King's River pyrg, and lay waste to traditional territories still used by people from the Fort McDermitt reservation and the local ranching and farming communities.

The Campaign to Protect Thacker Pass

They claim this is an "environmentally sustainable" project. We disagree, and we mean to stop them from destroying this place.

Thus far, our work has been focused on outreach and spreading the word. For the first two weeks, there were only two of us here. Now word has begun to spread. The campaign is entering a new stage. There are new opportunities opening, but we must be cautious.

How Corporations Disrupt Grassroots Resistance Movements

Corporations, faced with grassroots resistance, follow a certain playbook. We can look at the history of how these companies respond to determine their strategies and the best ways to counteract them.

Corporations like Lithium Americas Corporation generally do not have in-house security teams, beyond basic security for facilities and IT/digital security. Therefore, when faced with growing grassroots resistance, their first move will be to hire an outside corporation to conduct surveillance, intelligence gathering, and offensive operations.

Private Military Corporations (PMCs) are essentially mercenaries acting largely outside of government regulation or democratic control. They are hired by private corporations to assist in their interests and act as for-hire businesses with few or no ethical considerations. Some examples of these corporations are TigerSwan, Triple Canopy, and STRATFOR.

PMCs are often staffed with U.S. military veterans, and employ counterinsurgency techniques and skills honed during the invasions of Iraq and Afghanistan, or other military operations. And in many cases, these PMCs collaborate with public law enforcement agencies to share information, such that law enforcement is essentially acting as a private contractor for a corporation.

Disruption Tactics Used by Corporate Goon Squads

PMCs can be expected to deploy four basic tactics.

1. **Intelligence Gathering**

First, they will attempt to gather as much information on protesters as possible. This begins with what is called OSINT — Open Source Intelligence. This simply means combing through open records on the internet: Googling names, scrolling through social media profiles and groups, and compiling information that is publicly available for anyone who cares to look.

Other methods of information gathering are more active, and include physical surveillance (such as flying a helicopter overhead, as occurred today), signals intelligence (attempting to capture cell phone calls, emails, texts, and website traffic using a device like a Stingray also known as an IMSI catcher), and infiltration or human intelligence (HUMINT). This last is perhaps the most important, the most dangerous, and the most difficult to combat.

2. **Disruption**

Second, they will attempt to disrupt the protest. This is often done by using the classic tactics of COINTELPRO to plant rumors, false information, and foment infighting to weaken opposition.

During the protests against the Dakota Access Pipeline, one TigerSwan infiltrator working inside the protest camps wrote to his team that

"I need you guys to start looking at the activists in your area and see if there are individuals who are vulnerable. They're broke, always talking about needing gas money or whatever. Maybe they're disillusioned, depressed a little. Life is fucking them over. We can buy them a bus ticket to any camp they want if they're willing to provide intel. We win no matter what. If they agree to inform for pay, we get intel. If they tell our pitchman to go f*** himself/herself, the activist will start wondering who did take the money and it'll cause conflict within the activist groups and it won't cost us anything."

In 2013, there was a leak of documents from the private intelligence company STRATFOR, which has worked for the American Petroleum Institute, Dow Chemical, Northrup Grumman, Coca Cola, and so on. The leaked documents revealed one part of STRATFOR's strategy for fighting social movements. The document proposes dividing activists into four groups, then exploiting their differences to fracture movements. "Radicals, idealists, realists and opportunists [are the four categories]," the leaked documents state. "The Opportunists are in it for themselves and can be pulled away for their own self-interest. The Realists can be convinced that transformative change is not possible and we must settle for what is possible. Idealists can be convinced they have the facts wrong and pulled to the Realist camp. Radicals, who see the system as corrupt and needing transformation, need to be isolated and discredited, using false charges to assassinate their character is a common tactic."

As I will discuss later on, solidarity and movement culture is the best way to push back against these methods.

Other examples of infiltration and disruption have often focused on:

- Increasing tensions around racist or sexist behavior
- Targeting individuals with drug or alcohol addictions to become informants
- Using sex appeal and relationship building to get information
- Acting as an "agent provocateur" to encourage protesters to become violent, even to the point of supplying them with bombs, in order to secure arrests
- Spreading rumors about inappropriate behavior to sew discord and mistrust

3. **Intimidation**

The third tactic used by these companies is intimidation. They will use fear and paranoia as a deliberate form of psychological warfare. This can include anonymous threats, shows of force, visible surveillance, and so on.

4. **Violence**

When other methods fail, PMCs and public law enforcement will ultimately resort to direct violence, as we have seen with Standing Rock and many other protest movements.

As I have written before, colonial states enforce their resource extraction regimes with force, and we should disabuse ourselves of notions to the contrary. Vigilante violence is also always a concern. When people seek to defend land from destruction, men with guns are usually dispatched to arrest them, remove them from the site, and lock them in cages.

How to Resist Against Surveillance and Repression

There are specific techniques we can deploy to protect ourselves, and by extension, protect the land at Thacker Pass. These techniques are called “security culture.” Security culture is a set of practices and attitudes designed to increase the safety of political communities. These guidelines are created based on recent and historic state repression, and help to reduce paranoia and increase effectiveness.

Security culture cannot keep us 100% safe, all the time. There is risk in political action. But it helps us manage risks that do exist, and take calculated risks when necessary to achieve our goals.

The first rule of security culture is this: be cautious, but do not live in fear. We cannot let their intimidation be effective. Creating paranoia is a key goal for PMCs and other repressive organizations. When they make us so paranoid we no longer take action, reach out to potential allies, or plan and carry out our campaigns, they win using only the techniques of psychological warfare. When we are fighting to protect the land and water, we are doing something righteous, and we should be proud and stand tall while we do this work.

The second rule of security culture is that solidarity is how we overcome paranoia, snitchjacketing, and rumor-spreading. We must act with principles and in a deeply ethical and honorable way. Work to build alliances, friendships, and trust—while maintaining good boundaries and holding people accountable. This is the foundation of a good culture.

In regards to infiltration, security culture recommends the following:

1. It’s not safe nor a good idea to generally speculate or accuse people of being infiltrators. This is a typical tactic that infiltrators use to shut movements down.
2. Paranoia can cause destructive behavior.
3. Making false/uncertain accusations is dangerous: this is called “bad-jacketing” or “snitch-jacketing.”
4. Build relationships deliberately, and build trust slowly. Do not share sensitive information with people who don’t need to know it. There is a fine line between promoting a campaign and sharing information that could put someone at risk.
5. Good security culture focuses on **identifying and stopping bad behavior.**
6. Do not talk to police or law enforcement unless you are a designated liaison.

Secure communications are an important part of security culture.

Here are some basic recommendations to secure your communications.

1. Email, phone calls, social media, and text messages are inherently insecure. Nothing sensitive should be discussed using these platforms.
2. Preferably, use modern secure messaging apps such as Signal, Wire, or Session. These apps are free and easy to use.
3. We recommend setting up and using a VPN for all your internet access needs at camp. ProtonVPN and Firefox VPN are two reputable providers. These tools are easy to use after a brief initial setup, and only cost a small amount. Invest in security.

We must also remember that secure communications aren't a magic bullet. If you're communicating with someone who decides to share your private message, it's no longer private. Use common sense and consider trust when using secure communications tools.

Security culture also warns us not talk about some sensitive issues, including:

- Your or someone else's participation in illegal action.
- Someone else's advocacy for such actions.
- Your or someone else's plans for a future illegal action.
- Don't talk about illegal actions in terms of specific times, people, places, etc.

Note: Nonviolent civil disobedience is illegal, but can sometimes be discussed openly. In general, the specifics of nonviolent civil disobedience should be discussed only with people who will be involved in the action or those doing support work for them. It's still acceptable (even encouraged) to speak out generally in support of monkeywrenching and all forms of resistance as long as you don't mention specific places, people, times, etc.

Conclusion

Security is a very important topic, but is challenging. There are so many potential threats, and we are not used to acting in a secure way. That's why we are working to create a "security culture"—so that our communities of resistance are always considering security, assessing threats, studying our opposition, and creating countermeasures to their methods.

This article is only a brief introduction to the topic of security culture. Moving forward, we will be providing regular trainings in security culture to Protect Thacker Pass participants.

Most importantly, do not let this scare you, and do not be overwhelmed. Simply take one security measure at a time, begin to study it, and then implement better protocols one by one. We use the term "security culture" because security is a mindset that should be developed and shared.

Resources:

- https://ssd.eff.org/en/module/attending-protest
- https://deepgreenresistance.org/en/get-involved/security-culture
- https://www.youtube.com/playlist?list=PLF2F327D60839F552
- https://ssd.eff.org/
- https://securityinabox.org/en/
- https://freedom.press/training/mobile-security-protest-preparation-tips-activists/

Recommended topics of study:

- Device encryption

- Physical security / self-defense
- Secure email providers
- Two-factor authentication
- “Evil maid” and other physical attacks
- COINTELPRO

Max Wilbert is an organizer, writer, and wilderness guide.
He is the author of two books, most recently: *Bright Green Lies: How the Environmental Movement Lost Its Way and What We Can Do About It* (2021 — with Derrick Jensen and Lierre Keith).