WINTERHORN:
12 TECHNIQUES

The twelve techniques you use when playing WINTERHORN are all pulled from real life and are being used all over the world right now. I encourage you to learn more about these and other techniques governments employ to suppress dissent and control their citizens, and to take what you learn and use it to make yourself and the groups you care about more aware and resilient. Below, I've offered an historical example of each of the techniques, followed by a few directed questions.

Jason Morningstar
Durham, North Carolina, USA
2 December 2017

SURVEILLANCE
FRONT GROUP
DISINFORMATION
RECRUITMENT
INTERCEPTION
MANIPULATION
INFILTRATION
BLACK BAG JOB
INTIMIDATION
BAD JACKETING
VANDALISM
VIOLENCE

104-R NC Hwy 54 Bypass #169
Carrboro NC 27510

ISBN: 978-1-945633-05-8

SURVEILLANCE

Surveillance is the bedrock of government intrusion and control. It can take the form of discrete monitoring and observation, either physically or electronically, or it can be more overt (in which case it drifts into other techniques, like manipulation or intimidation).

Because of his sympathy for, and sometimes membership in, peace and social justice activist groups, Albert Einstein became a target of FBI surveillance. His phones were tapped and his mail was read in an effort to tie him to Soviet espionage and get him deported. Einstein's file grew to 1800 pages, and a parallel Immigration and Naturalization investigation, prompted by the FBI, lasted five years.

The NSA's PRISM program, as revealed by Edward Snowden, is an extreme example of surveillance — global in scale and reach. Partnering with the Australian Signals Directorate, Government Communications Headquarters of the UK and Algemene Inlichtingen en Veiligheidsdienst of the Netherlands, as well as Microsoft, Google, Apple and Facebook, PRISM collected (and, likely, collects) targeted Internet communications through secret treaties and equally secret FISA court orders.

- How are you being observed in your daily life?
- How would you know if you were a target of focused surveillance?
- What steps can you take to avoid or disrupt surveillance?

FRONT GROUP

It is convenient and often effective to fund organizations, sometimes created by the government completely, to advocate for specific policies, or draw activists away from more effective or radical groups, or simply to muddy the water.

South Africa's apartheid government spun up many front groups, including an entire newspaper (The Citizen). The Federal Independent Black Alliance was a conservative black advocacy group. The International Freedom Foundation, based in Washington, fought sanctions and funneled aid to UNITA in Angola. Veterans for Victory was created as a counterbalance to the campaign to end universal conscription. Jeugkrag (Youth for South Africa) was funded by South African military intelligence. All these groups were specifically engineered to aid the apartheid government and promote its policies.

- How can you tell if an organization is legitimate or a front?
- Is it possible for a group to do useful work and be a governmental front group?
- When you identify a front group, what can you do about it?

DISINFORMATION

Governments can use disinformation both to change the conventional narrative on a topic and to disrupt activism by sowing doubt and confusion. "Fake news" delegitimizes journalism and objective truth itself, something that is very useful if you need to tell lies.

On 5 September 2010, the UK's Independent newspaper published a puff piece called "Valentina Matviyenko: Meet Russia's Thatcher". Matviyenko, unelected Mayor of Leningrad, was a crony of Putin, and the fawning piece raised her stature within Russia, where foreign press coverage carries more weight than notoriously corrupt local journalism. It didn't escape the notice of a single Leningrader that the article was pure *zakazukha*, however. "Zakazukha" is a Russian word for paying for favorable media coverage, which has transformed into paying for custom-tailored journalism— fake news. The Independent's Matviyenko article was built to please Putin, who was in the process of cutting his rival Russian oligarchs down to size. And the Independent newspaper, based in London, was (and is) owned by Alexander Lebedev, former KGB agent and current oligarch.

- Who is lying to you right now?
- How can you identify disinformation?
- What can you do to both prevent and mitigate disinformation campaigns directed at you?

RECRUITMENT

Recruitment goes hand in hand with infiltration, and each presents trade-offs. A confidential informant is more likely to be trusted and doesn't need to grow into the network of the targeted organization, but may lack skill and experience in matters the government cares about. Informants, however, are often an inexpensive and rapid way "into" a group.

The FBI's offensively named Ghetto Informant Program (GIP) was designed to recruit confidential informants close to "key Black extremists" like Martin Luther King, Jr., Floyd McKissick, Malcolm X, Stokely Carmichael, and many others. Informants orbiting these figures kept the Bureau appraised of their movements, plans, attitudes, and internal conflicts for a decade, in some cases fomenting dissent and animosity between them. FBI informants creating friction between Malcolm X and Elijah Mohammed was at least a contributing factor in the former's assassination.

- How can you maintain a community of trust and also be resilient to informers?
- How can you identify informers within your organization?
- What do you do when an informer has been identified?

INTERCEPTION

Gathering signals intelligence, while technically complex, offers a hands-off way to learn details about a target that would be nearly impossible to gather in any other way. And as technology becomes ubiquitous, so do the opportunities for listening in.

In 2004 and 2005, more than one hundred mobile phones were tapped in Athens, Greece, primarily those belonging to Greek politicians and civil servants. The eavesdroppers, later identified as American NSA employees, listened in on the Prime Minister and key officials in the Ministries of Defense, Foreign Affairs, and Public Order, as well as ruling and opposition party members. Due to clumsy tradecraft and diligent investigation, 14 prepaid phone cards were traced back to the US embassy in Athens, and a SIM card registered to the US Embassy made calls to communities around the NSA headquarters in Maryland.

- How do you communicate now?
- What are the weak links in your methods of communication?
- How can you harden your communication channels against interception?

MANIPULATION

Like vandalism, manipulation can be viewed as a focused form of intimidation. By targeting the people surrounding the subject of an investigation, both fear and doubt can be generated. If a subject's entire world is frightened, angry, or suspicious, they are likely to make poor decisions.

Examples of overt manipulation are easy to find. In 2010 Republican Sinn Féin, a group politically tied to the Continuity Irish Republican Army, complained that armed, masked British soldiers from the Special Reconnaissance Regiment were conducting surveillance in Lurgan, County Armagh using unmarked white vans. The targeted estates, home to the families of many IRA prisoners, were subsequently blanketed by police who invoked the "stop and search" powers of Article 44 of the Terrorism Act indiscriminately.

- Are you a good candidate for manipulation? Are those close to you vulnerable?
- How will you know if those around you are being manipulated?
- What actions can you take if you or those close to you are being manipulated?

INFILTRATION

Inserting government operatives within activist groups is a high risk and high reward technique. Having someone "on the inside" can be enormously valuable for understanding a group's plans and social dynamics, but when it goes wrong, it can go very wrong.

Just a few examples of infiltration in the United State after consent decrees forbidding surveillance were lifted in 2003:

2004: The New York Police Department infiltrates protest groups and arrests over 1800 people in advance of the Republican National Convention.

2007: The Maryland State Police infiltrate groups of peace activists statewide.

2008: The Joint Terrorism Task Force infiltrates vegan potlucks in Minneapolis in advance of the Republican National Convention.

2012: Chicago police infiltrate Chicago Action Medical, volunteer protest street medics.

2013: Police in Washington, DC infiltrate peace groups in the city.

2017: Police in Washington, DC infiltrate protest groups prior to the Presidential inauguration.

- How can you remain open to newcomers and also resilient to infiltration?
- How can you identify infiltrators within your organization?
- What do you do when an infiltrator has been identified?

BLACK BAG JOB

The archetypal black bag job involves surreptitious entry to observe or copy records in situ, but it can be part of a constellation of intimidation (by leaving evidence of a visit) and surveillance (by planting bugs) as well.

In October 1972, members of the Royal Canadian Mounted Police broke into the offices of the Agence de Presse Libre du Québec, a radical leftist news agency. They stole everything from subscription lists to the clipping morgue, as well as bank records. The burglary paralyzed the operations of the APLQ, a completely legal organization. When the involvement of the national police in the break-in was revealed, the RCMP officer who had authorized it — and who had been promoted immediately after its success — was assigned to prepare the official report. And this wasn't the first RCMP black bag job — two years earlier the offices of Praxis, a research firm working for welfare rights advocates, had been burgled and set on fire after its files were stolen. These later turned up as a blacklist of sympathetic civil servants that was widely circulated.

- What are your physical and electronic security like? Where do you keep your records?
- Will you be able to tell if you've been burgled or hacked?
- What steps can you take to harden your operations security?

INTIMIDATION

The ability of a far-reaching and monolithic government to harass and terrify is well understood, and direct threats can, often, be both plausibly denied and chillingly effective at controlling behavior.

The Russian technique of *Kompromat* involves assembling a dossier of compromising material on the target using anything from doctored photos to cyber crime to surveillance and honey pots (setting up the target with prostitutes, for example). Once the target is entrapped, they either become an asset or are ruined, and either way the state wins.

A classic example: In January 1999, Russian Prosecutor General Yury Skuratov was immersed in a bribery investigation involving a Swiss bank and the Russian President, Boris Yeltsin. He was called to the Kremlin and shown a grainy videotape by Yeltsin's chief of staff. It showed someone who looked a lot like him having sex with two women. Skuratov claimed it was a fake, but resigned anyway.

- Would you be easy to intimidate? Why?
- Could you be transparent about your life and behavior, however mortifying, if necessary to prevent intimidation?
- What actions can you take if you are being intimidated?

BAD JACKETING

The FBI loved, and probably loves, bad jacketing as a way to turn groups against one another. By inserting a false, incriminating narrative and allowing it to grow organically, the source becomes lost and the rumor gains an air of authenticity. Successful bad jacketing can stir up paranoia and suspicion and lead to everything from community implosion to internecine violence.

An FBI proposal related to the bad jacketing of Student Nonviolent Coordinating Committee leader Stokely Carmichael by a Special Agent-in-Charge in New York to Director Hoover, issued on 10 July 1968:

"It is recommended that consideration be given to convey the impression that CARMICHAEL is a CIA informer. One method of accomplishing this would be to have a carbon copy of informant report reportedly written by CARMICHAEL to the CIA carefully deposited in the automobile of a close Black Nationalist friend. … It is hoped that when the informant report is read it will help promote distrust between CARMICHAEL and the Black Community … It is also suggested that we inform a certain percentage of reliable criminal and racial informants that "we have heard from reliable sources that CARMICHAEL is a CIA agent." It is hoped that these informants would spread the rumor in various large Negro communities across the land."

This proposal was approved within 24 hours, by the way. And 18 months later, Huey P. Newton openly accused Carmichael of being a CIA agent.

- What level of trust exists within your activist community?
- How can you tell if incriminating or inflammatory information is legitimate or fabricated?
- How can you strengthen an organization against bad jacketing?

VANDALISM

In many ways vandalism as politically motivated violence can be viewed as a subset of intimidation. The destruction and defacement of property sends a clear signal while creating unease and confusion. Senseless, random vandalism also occurs, after all.

On 22 March 2010, the Danville, Virginia Tea Party Chairman and other organizers posted a home address they thought belonged to US Representative Tom Perriello, inviting their members to stop by and express their anger at the Congressman over his affirmative vote on a health care bill (the home belonged to Perriello's brother). That night, according the subsequent FBI investigation, someone entered the home's screened in porch and severed a line leading to a propane tank. Perriello's brother smelled the leaking propane before anyone was hurt.

- What is your physical security profile?
- How can you make yourself and the organizations you care about unattractive targets for vandalism?
- What response can you make to acts of politically-motivated vandalism?

VIOLENCE

Violence — at the hands of government agents or through proxies — is an extreme and often ineffective technique. The blowback from such behavior often emboldens survivors and provides concrete evidence that solidifies resistance. This is, of course, cold comfort to the people who are terrorized, tortured or killed.

On 19 January 2010, Mahmoud Al-Mabhouh, co-founder of the Izz ad-Din al-Qassam Brigades, the military wing of Hamas, was murdered in Dubai in an elaborate operation that involved at least 26 operatives using stolen and forged passports. Al-Mabhouh was drugged and electrocuted in his hotel room, and the entire team escaped. No one ever claimed responsibility but it is widely assumed that Israel's Mossad was behind the extrajudicial killing — "widely assumed" in this case meaning yes, it was definitely Mossad.

- How can you stay safe while also moving and speaking freely?
- How can you prepare for acts of politically motivated violence?
- What response can you make to violence and terror?