Red Swarm: Hacktivist Praxis

June 2020

Table of Contents

Introduction

"*Man's dearest possession is life. It is given to him but once, and he must live it so as to feel no torturing regrets for wasted years, never know the burning shame of a mean and petty past; so live that, dying, he might say: all my life, all my strength were given to the finest cause in all the world——the fight for the Liberation of Mankind*"

- Nikolai Ostrovsky, "*How the Steel Was Tempered*"

The world in the 21st century is dominated by an increasingly moribund and irrational economic system which values profit over people and the environment. The 'dotcom' bubble of the early 2000s, the financial crisis of 2008 and the crisis of the early 2020s have shown that the global capitalist system is unable to deal with the social and environmental antagonisms of our times. In such times, there has been an increased interest in bringing about an equitable and green post-capitalism – a higher mode of political economy.

In this situation, the most important issue is the question of how these aims will be practically achieved. While any solution will likely involve a diverse array of tactics and the participation of the masses, there is one form of direct action that has often been neglected by the left: that of 'hacktivism'.

Anonymous

"*Case met his first Modern two days after he'd screened the Hosaka's precis. The Moderns, he'd decided, were a contemporary version of the Big Scientists of his own late teens. There was a kind of ghostly teenage DNA at work in the Sprawl, something that carried the coded precepts of various short-lived sub cults and replicated them at odd intervals. The Panther Moderns were a soft head variant on the Scientists. If the technology had been available the Big Scientists would all have had sockets stuffed with microsofts. It was the style that mattered and the style was the same. The Moderns were mercenaries, practical jokers, nihilistic technofetishists.*"

- William Gibson, "*Neuromancer*"

Anonymous as a group has its origins in the website 4chan, a largely anonymous internet 'imageboard' with lax moderation standards. Before becoming a hacker collective 'Anonymous' had engaged in a number of online pranks and mass trolling campaigns. The history of Anonymous is interesting in and of itself, and you can read about it in detail in books like '*We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*' by Parmy Olson, '*Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*' by Gabriella Coleman, or Commander X (a.k.a. Christopher Doyon)'s semi-autobiographical work '*Behind The Mask: An Inside Look At Anonymous*'.

To briefly summarize that history: the turning point for Anonymous was 'Project Chanology', a protest by Anonymous against the Church of Scientology, which involved both online activities and real-life street action. It was at this point that the iconic Guy Fawkes masks became part of Anonymous. The influx of left-liberal activists into Anonymous at this point changed Anonymous from being a group of trollish nihilists into being a somewhat of a vigilante organization. Anonymous was also heavily involved in defending 'Wikileaks', a news organization known for leaking state secrets such as evidence of U.S. war crimes. The peak of Anonymous was from 2010 to 2011, a period that roughly coincided with the 'Arab Spring' and 'Occupy Wall Street' movements. At this point Anonymous was hacking the computers of various dictatorships in the middle east, as well as US corporate and governmental organizations. In mid to late 2011 and early 2012, many of the most technical hackers in Anonymous and 'LulzSec' were arrested (most were either in the UK or the US). This was due to one of the main 'LulzSec' hackers, Hector 'Sabu' Monsegur becoming an informant for the FBI after being arrested. Anonymous managed to continue operations up until 2015/2016, but their media profile greatly diminished. In fact, from 2015 to 2019, Anonymous seemingly ceased operations completely.

What did they get right and what did they get wrong? It is the responsibility of newer movements to learn from those that came before. Most hacker groups only last a few months and then quickly fade away, while the state actors and agencies they fight have decades of organizational experience in defeating such adversaries. A more considered, even 'academic' approach is needed. *[Just a quick note here, Anonymous was infiltrated and crushed by US federal law enforcement in 2011 and 2012. Do not join 'Anonymous' IRC chatrooms, etc. today unless you want to be put on a list. Use other methods and venues for meeting/recruiting likeminded people. The 'original' members of Anonymous mostly went to prison or quit, what remains today are largely US law enforcement and other state actors claiming the label]*

What went wrong with Anonymous:

1. A lack of ideological coherence

Anonymous was a bizarre mishmash of apolitical trolls, cyberpunks, liberals, libertarians, ironic racists, and far-left types. Anonymous never had a single coherent ideology and therefore never had a clear vision of what types of targets it was supposed to go after.

2. Lack of planning and strategy

According to Commander X, "*For those wondering how Anonymous begins a major Operation, it usually starts with righteous indignation bordering on group outrage*". In other words, many Anonymous Operations were usually spontaneous and not pre-planned, being based on members of Anonymous hyping themselves up over an injustice on IRC chat. While this has the advantage of choosing targets that are popular (being the subject of popular outrage), it has the downside of leaving no time to plan. Breakout group LulzSec/AntiSec had a bit more planning.

3. Telegraphing the Operation

It was often the case that Anonymous would tell the target of the operation that they were going to attack them. These would sometimes take the form of a press release, and sometimes in the form of a youtube video with some guy in a 'Guy Fawkes' mask using text to speech for some threatening message. This allowed time for the target to prepare.

4. Insecure Communications

The open model of using public IRC chats to coordinate allowed easy monitoring by law enforcement agencies such as the FBI. This was a problem most early 2010s social movements had in common (another example: 'Occupy Wall Street' and Twitter). There were also multiple instances where logs of private chats were leaked by members of LulzSec.

5. Weak Security Posture

While the members of LulzSec and Anonymous often took great pains to have moderately good technical security, they often had bad operational security. Most of the methods used to unmask them were not based on some highfalutin technical wizardry, but by a combination of relatively low tech network forensics and old fashioned detective work based on de-anonymizing personal details that members of these groups would admit to over IRC chat. This is easily seen by reading the court transcripts of the trials of members of LulzSec/AntiSec. There was also poor compartmentation of information in general.

6. Lack of Technicality and Amateurism

The members of Anonymous, even the more technical ones, were amateurs. Almost all of the techniques used by, for example, LulzSec, were nothing your average computer science sophomore couldn't whip up in a week (basic SQL injects, etc.). Even many of their DDOS attacks were based on people using a program (LOIC) that spammed requests at a website of their choosing. Because of the rise of CDNs and DDOS protection services like Cloudflare, these sorts of methods are no longer effective.

7. Organizational Learning

Groups like LulzSec were too short-lived to have any significant organizational learning. It is unclear to what extent this applies to the rest of Anonymous.

<u>What went right with Anonymous:</u>

1. Public/Media Relations

As corny as they are in retrospect, the various youtube videos, memes, and press releases of Anonymous were instrumental in its success, the point where the image of the Guy Fawkes mask became synonymous with hacking. You had events like the million mask march and celebrities like Russell Brand supporting Anonymous. You had lots of Guy Fawkes masks at Occupy Wall Street as well. You also had penetration into pop culture in various movies and TV shows, such as 'Mr. Robot'. Raising the media profile of an organization is critical in winning it popular support. Jake 'Topiary' Davis was also an extremely skilled public relations operator for 'LulzSec', hyping up the group's popularity on twitter.

2. (Extremely) High Operational Tempo

The decentralized nature of Anonymous allowed it to decide to move against a target quickly, sometimes within hours. This allowed it to respond quickly to threats (such as when it moved against HB Gary Federal after it's CEO threatened to 'dox' them). During the so-called '50 days of lulz' LulzSec engaged in numerous high-profile hacks.

3. Unpopular Targets

Anonymous being a vigilante-style group helped with unpopular targets. It could respond quickly to a popular outcry against these targets and thereby win itself support from the public. LulzSec, the offshoot group, mostly had unpopular targets but occasionally got it wrong due to the random nature of their mayhem.

Organizational Models: Tradeoffs

There has been a failure on the part of social movements to learn from past, whether that be the documented repression of the Black Panther Party in the 1960s, or Occupy Wall Street and Anonymous in the early 2010s. What little reflection there is relies exclusively on left-wing sources. Any serious analysis of past movements must draw on both left wing and bourgeois literature. One useful framework of analysis is that developed by Blake William Mobley, a RAND corporation political scientist and former counterintelligence analyst for the Central Intelligence Agency.[1]

Leftist hacktivists must understand the tradeoffs involved in any clandestine organization, as per Mobley's model:

- Hypothesis 1(A): A [group] with a tight command and control structure, relative to a group with a loose command structure, will have superior counterintelligence training and compartmentation.
- Hypothesis 1(B): A [group] with a tight command and control structure, relative to a group with a loose command structure, will be more vulnerable to its adversary's efforts to develop high-level penetrations and exploit the group's standardized counterintelligence procedures.
- Hypothesis 2(A): A [group] with popular support, relative to one without popular support, will have greater counterintelligence support from the local population.
- Hypothesis 2(B): A [group] with popular support, relative to one without popular support, will be more likely to expose sensitive information about its personnel and operations through its efforts to generate and maintain popular support.
- Hypothesis 3(A): A [group] with controlled territory, relative to one without territory, will have superior communications security, physical security and counterintelligence vetting.
- Hypothesis 3(B): A [group] with controlled territory, relative to one without territory, will be more vulnerable to its adversary's efforts to track the group's gross financial, logistical and personnel movements into and out of the controlled territory.

Mobley analyzes several clandestine (terrorist) organizations and classifies them using this model. For Mobley, the independent variables involved are:

- Organizational Structure (OS), being either tightly controlled and centralized, or loosely controlled and decentralized.
- Popular Support (PS), whether or not the group has popular support.
- Controlled Territory (CT), whether or not the group exclusively controls geographical territory.
- Adversary Capability (AD), the strength/organization of their adversary.

According to Mobley, these four core variables predict a number of other outcomes/dependent variables:

- Standardized CI Training for All Members (ST)
- Uniform CI Methods Across the Organization (UM)
- CI Support from Local Population (LS)

- Damaging CI Exposure Through Media Contact (ME)
- Sophisticated Communications Security (CS)
- Vetting and Counterespionage Investigation (VC)

If we analyze 'Anonymous' using this framework, we get the following:

- OS – Anonymous had a loose, decentralized nature.
- PS – Anonymous had lots of supporters or 'cheerleaders' online.
- CT – Anonymous was globally distributed and therefore never had enough geographically co-located support to have any controlled territory, and in any case since most of it's core members were in the UK or US, so the idea that a bunch of hackers could make a western government cede territory, even temporarily, is totally out of the question.
- AD – Anonymous' adversaries were corporations and government agencies. The US security state (NSA, CIA, FBI, etc.) in particular is obviously a very strong adversary.

These taken together would mean that Anonymous, taken as a whole, is a 'Type 14' organization, which predicts: counterintelligence support from 'local' population, and damaging counterintelligence exposure through media contact. On the negative side, it predicts a lack of standardized training, poor communications security, and poor vetting/counter-espionage. Anonymous/LulzSec's lack of 'local' CI support can be explained by the fact that even though Anonymous had lots of supporters, they were not located in one particular 'local' neighborhood. LulzSec certainly had a high operational profile, which is eventually what brought law enforcement down on them.

What would have happened if Anonymous would have been a centralized organization with a formal hierarchy and compartmentation of information? Well if we just adjust that one variable, centralized organization, we get a 'Type 6' organization, which predicts standardized and uniform CI training, increased communications security, vetting, and counterespionage abilities.

Even if we assume that a more hierarchical organization would result in less mass participation (via the IRC channels) and therefore lower popular support, we would still be able to classify Anonymous as a 'Type 2' organization which would still retain the advantages of standardized/uniform training, communications security, vetting, etc., at the cost of a lower media profile.

Mobley's central thesis: "*Contrary to popular belief… hierarchical and tightly organized [organizations] are frequently superior to decentralized or 'network' [organizations] in their counterintelligence capabilities, and therefore are in many cases better suited for long-term survival.*" [2]

Mobley's Model (table)

Variables and Hypothesized Effects

Type	Independent Variables				Dependent Variables					
	OS	PS	CT	AD	ST	UM	LS	ME	CS	VC
1	+	-	-	-	=	+	-	-	=	=
2	+	-	-	+	+	+	-	-	+	+
3	+	-	+	-	+	+	-	-	+	+
4	+	-	+	+	+	+	-	-	+	+
5	+	+	-	-	+	+	+	+	=	=
6	+	+	-	+	+	+	+	+	+	+
7	+	+	+	-	+	+	+	+	+	+
8	+	+	+	+	+	+	+	+	+	+
9	-	-	-	-	-	-	-	-	-	-
10	-	-	-	+	-	=	-	-	-	-
11	-	-	+	-	=	-	-	-	=	=
12	-	-	+	+	+	=	-	-	+	+
13	-	+	-	-	-	-	+	+	-	-
14	-	+	-	+	-	=	+	+	-	-
15	-	+	+	-	=	-	+	+	+	+
16	-	+	+	+	+	=	+	+	+	+

Independent and Control Variables		Inputs	
OS	Organizational Structure	+	Tight
		-	Loose
PS	Popular Support	+	High
		-	Low
CT	Controlled Territory	+	Yes
		-	No
AD	Adversary Capability	+	High
		-	Low

Dependent Variables	
ST	Standardized CI Training for All Members
UM	Uniform CI Methods Across the Organization
LS	CI Support from Local Population
ME	Damaging CI Exposure Through Media Contact
CS	Sophisticated Communications Security
VC	Vetting and Counterespionage Investigation

Hypothesized Outcomes	
=	No Effect
-	Less Likely
+	More Likely

M.S.S.P. (Maintain Strong Security Posture)

"*maintaining a strong security posture for prolonged periods of time is an extremely stressful and difficult act. Operatives working for the intelligence agencies have a significantly easier time of it than those on the other side of the protection of the state: e.g. their agents; hackers; terrorists, and narcos. The "legal" operatives have peers that they can confide in and unwind with thanks to the protections of the nation state. The true clandestine agents must be guarded with their peers, the public and the adversary. Any peer might be an informant, either now or in the future. Opening up and being friendly with their peers is part of what lead to the unraveling of the lulzsec hacker group.*"

- The Grucq, "*Hacker OPSEC with The Grugq*"

Operations security, also known as 'operational security' or 'OPSEC' is often neglected by hackers, or at the very least, not given enough thought. Maintaining strong security posture is stressful and it slows down the work of an organization: yet, it is essential if members of an organization want to have even a chance at evading the state security apparatus.

OPSEC, is to a large extent, non-technical. It has less to do with computers and more to do with 'tradecraft' i.e. the skills that intelligence agencies and spies have practiced from time immemorial. Hacker/security researcher 'The Grucq' gives ten rules for Hacker OPSEC [3]:

1. Never reveal your operational details
2. Never reveal your plans
3. Never trust anyone
4. Never confuse recreation and hacking
5. Never operate from your own house
6. Be proactively paranoid, it doesn't work retroactively
7. Keep personal life and hacking separated
8. Keep your personal environment contraband free
9. Don't talk to the police
10. Don't give anyone power over you

Some examples of what not to do

These are excerpts from the trial transcripts of anarcho-communist 'AntiSec' hacker Jeremy Hammond:

d. In a chat with CW-1 on or about July 21, 2011, an individual using the alias "Anarchaos," later identified as the defendant, told CW-1 that he had been "arrested for weed and did two weeks in county jail." Later in that same chat that individual said: "Don't tell anybody cause it could compromise my identity but I am on probation… I've done time before though it's all cool."

This is a violation of rule #3. Do not trust people on the internet with this sort of information under any circumstance.

f. In a chat on or about July 31, 2011, at approximately 3:30 a.m., an individual using the alias "POW,", later identified as the defendant, stated that "dumpster diving is all good i'm a freegan goddess." I know based on my investigation that "freegans" are individuals who practice eating and reclaiming food that has been discarded as part of an anti-consumerist movement. According to the Chicago law enforcement authorities whom I have spoken to who have conducted surveillance of JEREMY HAMMOND, the defendant, in the course of their investigations of HAMMOND since 2005, HAMMOND is a "freegan." In conducting surveillance, agents have seen HAMMOND going into dumpsters to get food.

This is a violation of rule #7 – keep hacking and personal life separate.

(iv) The FBI in Chicago obtained information in the course of a separate investigation that HAMMOND may have been involved in hacks into the website of a white supremacist organization. According to that investigation, various IP addresses used to access the reported hacked accounts were connected to HAMMOND.

Rule #5 – never operate from your home. Although to be fair, in Hammond's case, he was on 'enhanced probation' at the time and under a curfew, so leaving his home was difficult. In this case it may have been better to abstain from hacktivism for a while.

37. During the course of the physical surveillance, FBI agents detected public signals broadcast from a wireless router (the "ROUTER") which, based on measurements of signal strength and the use of directional antennas, they determined was located inside and towards the rear of the CHICAGO RESIDENCE… One of the MAC addresses at the CHICAGO RESIDENCE was identified as belonging to an Apple computer (the "Apple MAC Address"). The defendant, using the alias "sup_g," and CW-1 have discussed the fact that the defendant used a "macbook," an Apple laptop. When the Apple MAC Address was initially identified as active at the CHICAGO RESIDENCE, there were no indications that any other devices were connecting to the ROUTER; moreover, CW-1 reported to me that the defendant was online at that time.

b. An FBI TOR network expert analyzed the data from the Pen/Trap and was able to determine that a significant portion of the traffic from the CHICAGO RESIDENCE to the internet was TOR-related traffic. The Apple MAC Address was the only

MAC address at the CHICAGO RESIDENCE that was connecting to known TOR network IP addresses. The defendant, using the alias "yohoho," has discussed with CW-1 that he used the TOR network. For example in a chat over a jabber service on or about February 2, 2012, at approximately 5:22 a.m., "yohoho" said that he could not play youtube videos because "it won't play over tor." On February 6, 2012 at approximately 4:31 p.m., "yohoho" complained that "tor's always up and down."

Violations of Rule # 1 – never reveal operational details. Don't reveal which, if any VPN you are using. Don't reveal if you are using TOR. This is mainly circumstantial evidence but that is bad enough.

Personally identifying information could be things like weight, height, age, race, nationality, language (and use of a non-standard US keyboard), participation in real life political events, and even weather. Keeping regular hours also can be identifying because it gives a hint at what time zone you live in. Do not include any hints to your real life identity or even hobbies in any alias you create. Do not keep logs of anything. If you need information you copy and paste it into a text file. Logs are incriminating. Do not mention your job, hobbies, or involvement in activist groups. Do not use the regular internet while chatting over TOR/VPN etc anonymously.

Do not use twitter, facebook, google/youtube, or any major social network as these are all extensions of the US/UK security state. Do not post anything on a major social network that you would not feel comfortable sending directly to the FBI. If using a VPN and TOR in conjunction, go from TOR to VPN, NEVER the other way around. Only pay for VPNs with a privacy oriented cryptocurrency such as 'Monero'. It goes without saying but never give the VPN service your real IP by directly connecting to them, or your real customer information/name/address. Don't trust a VPN service not to hand over logs or anything else to law enforcement. If you read about the history of LulzSec [4], it is evident that one of the main reasons they got owned is that law enforcement forced their VPN provider "HideMyAss" to hand over their logs revealing their real IP addresses.

With regards to a VPN recommendation, you have to do your own research, but the following VPNs have a history of logging and cooperating with US/UK law enforcement:

- HideMyAss
- PureVPN
- IPVanish
- RiseupVPN (riseup.net)

Obviously, using one of these services is not recommended. Note that even if you use a VPN and they don't collect or hand over logs, your VPN also has an Internet Service Provider which can can hand over logs. This can be used to correlate your activity (you connecting to a VPN, then a VPN connecting to a website). This is rare but still theoretically possible. A VPN alone without TOR works for torrenting movies, but is not sufficient for hacktivist security.

You can connect using a mobile uplink or coffee shop wifi (never from home). Mobile uplinks are better but again, be careful about how you buy them and how that may be linked back to you (CCTV, credit card, etc). Finally, do not use your phone for any hacktivist related activities (when you go to the coffee shop for example) since phones can track your movements in physical space and are often used by law enforcement to do this. This was used in the 2020 George Floyd protests to identify and arrest protestors who stayed out after curfew. Even though their faces were concealed, their phones gave away their identities.

Developing security consciousness is a process that takes time. Don't engage in any hacktivism-related activities until you master it - "*Amateurs practice until they get it right, professionals practice until they can't get it wrong*".

Other notes on general computer security:

- Fully encrypt your hard drive – This sounds simple, but so many hackers have not done this and been owned because of it. All three major operating systems have methods of doing full disk encryption (although as a 'real hacker' you should be using Linux). Use an encryption password that is, at a minimum, 20 characters long and consists of random letters, numbers, and symbols. Alternatively, use a passphrase/sentence. Do not use anything from song lyrics or pop culture when using a passphrase. Use *at least* six words (consisting of at least five letters each) in the phrase, which should be nonsense and not found anywhere on the internet or in pop culture. These are much easier to memorize and therefore can be much, much longer, which is good. Your encryption password should be as long as is possible and therefore as hard to crack as possible, but you still need to remember it.
- Always turn off your computer – So many hackers have been owned because they didn't turn off their computer when law enforcement came and so their computer got live imaged by forensic software, and was not even locked, so they had free access to it! No amount of encryption can help you if an adversary has access to a running and non-locked computer. If you are going to sleep, shut down your computer. If you are taking a shower, shut down your computer. If you are answering a knock on your door from the pizza delivery guy, turn off your computer, because it might be NYPD/Scotland Yard/NCA/FBI/etc. Triple check that your computer is fully turned off because then at least they will have to deal with encryption rather than just creating a live forensic image of your computer.
- Keep all info on a single disk. If you can help it, keep all hacktivism-related activity on a single SD card. They are cheap so you won't sweat destroying one in a bout of paranoia. You should encrypt these too (actually encrypt any electronics you have from SD cards, to USB thumb drives, to external hard drives, etc.).
- Physically destroy your electronics when you are about to be caught – Again, there are a lot of hackers who understand this but don't practice it. Smash it with a sledgehammer, microwave the SD card on wax paper 'Mr. Robot' style (or flush it down the toilet if you're really in a hurry), take it out to the back yard and pour kerosine on it and light it on fire, just make sure that the physical hardware is 100%, irreparably, physically, destroyed. You can't do digital forensics on an ash pile. Do this proactively (which is why the SD card is a good idea, unless you are loaded with cash to keep destroying full hard drives), by the time the FBI is bursting in your door, it will be too late. Most people know when they are about to get got, and if you have a random cast of 'village people'

looking folks hanging out around your apartment (undercover agents) you should probably start thinking about flushing that SD card. This is a problem with a lot of hackers, they don't have the common sense that any two bit meth addict has to get rid of the evidence, and not to 'shit where you eat'. This won't help you completely because if they know where you live then that probably means they have your IP address, and enough evidence on network forensics + chat logs alone even without your hard drive, but that's no reason to make it easy. Also your computer could have additional logs and evidence to identify and incriminate your comrades, so thats a good enough reason to secure it, even if you are screwed personally.

- Don't buy stuff off the dark web, or sell stuff on the dark web – Half of all dark web marketplaces are fed honeypots being used to entrap people. In order to buy stuff off the dark web, you need to give them your name/address so they can mail the items to you, and when they get caught they hand over the database to the feds. Sometimes the FBI operates it for months after, collecting as much user data as possible. This is how they got Marcus "MalwareTech" Hutchins, because he sold malware on AlphaBay which was later seized by the FBI. DO NOT BUY OR SELL STUFF OFF DARK WEB CRYPTO MARKETS. THEY ARE OPERATED BY CRIMINALS WHO WILL 100% RAT YOU OUT IF AND WHEN THEY GET CAUGHT.
- One crime at a time – Not trying to be puritan here, but do not drink to excess or use drugs, even quasi legal ones like marijuana. Hackers have been caught this way before. Even if the hacking charges couldn't be proven, they got them on some unrelated drug charges because when the FBI raided their house they found weed. Part of how they flipped Sabu (aside from his kids) was that they got him on a bunch of petty crime charges like selling stolen credit cards on facebook (idiot). This is what caused him to snitch on LulzSec. If you're going to be a hacktivist, don't commit other crimes involving drugs, etc. or worse, be on actual probation like Hammond, (for a hacking conviction no less).
- Sanitize your social media – I recommend sanitizing your social media. Depending on how old you are, this is a process that could take months. Go back through gmail and find every single account with every single service or website you have ever used and try to delete them. They got the original Silk Road guy because he posted a question about the code for the Silk Road on stack overflow and also gave his real gmail account on some forum (which was his real first and last name). Imagine being a bitcoin billionaire and getting owned by a google search. Do not use any service from any tech company, especially American ones like google/youtube/facebook/twitter/instagram/etc. without evaluating it for privacy. Handing your information over to an American tech giant is essentially the same as handing it directly to the FBI/NSA. Switch from gmail to a more secure email provider like tutanota or protonmail. Tech companies usually take 3 to 18 months to delete your old data, if they ever do. Intelligence agencies like the NSA may keep stuff longer, if not forever, but there's nothing you can do about that. Try to be a social media ghost.

Insider Threats

An 'insider threat' (otherwise known as a 'mole', 'rat', 'snitch', or 'informant') is the single greatest problem your organization can face. No one knows this better than the state security agencies themselves, which is why they have a rigorous vetting process for people who want to join their organizations, including background checks and polygraphs.

Law enforcement and intelligence agencies aren't *that* smart. Thanks to television shows like 'CSI' people have the mistaken impression that your average police/FBI investigation relies on some highfalutin forensic wizardry: it doesn't. It's mostly a combination of basic detective work and getting people to inform on their colleagues. The internet, if anything, has made them even lazier.

Historically, almost all 'take downs' of hackers and hacker groups have been due to informants. In order to combat this, there must be several steps taken:

1. Compartment information and control of your organization such that there is no single central point of counterintelligence failure (i.e. structure your organization so that it cannot be taken down by a single mole in any one place).
2. Have a careful 'vetting' process so that people who are agents/informants, or are likely to become informants in the future, never join to begin with.
3. Eject suspected informants from the organization.

In 'traditional' revolutionary groups, informants (or suspected informants) are simply killed. However, this obviously cannot apply to most forms of hacktivism. Aside from the moral problem, there is the fact that if you are practicing good OPSEC, you don't know who your fellow hackers actually are. Politely ejecting the person from your organization for being a suspected informant (although you don't have to tell them why), or for repeated OPSEC violations, is the only solution.

To understand how to minimize the risks of informants, we have to understand why someone would become an 'informant' in the first place.

The Types of Informants

There are several 'types' of informants [6]:

1. Witness/Informant (a.k.a. "Cooperative Witness") - For the FBI, "Cooperative Witness" simply means informant. A witness/informant is someone who turns evidence for the prosecution after being arrested or experiencing some other 'defining event' from which there is no return.
2. Active Informant – Someone who is still embedded in the organization and is actively participating while relaying information back to their handler.
3. Source of Information – Technically not informants but third party tipsters (ex: VPN companies providing information on their customers, pawnbrokers, randos who call those crime hotlines if they "see something").
4. Jailhouse Informant – Otherwise known as a 'jailhouse snitch', a person who provides information on crimes from prison, often in hopes of reducing their sentence.
5. Unwitting Informant – Someone who gives information 'unwittingly' to an undercover agent without knowing their true identity.
6. Agent Provocateur – An informant or undercover agent that tries to bait people into committing crimes or attacking/not attacking certain targets.

The motivations of informants

There are several major motivations for informants [5][6]:

1. Money – Greed can be a motivation for people to turn into informants.
2. Ego – One of the more underestimated motivations is the need for someone to feel important or 'in command' of the situation. By becoming an informant, they feel as though they are somehow more 'in control' of the events that are happening than if they were just an ordinary member of the group.
3. Fear – In a hacktivist context, mostly the fear of incarceration dangled over a hacker who has been caught.
4. Revenge – Jennifer Emick, a former Anonymous/Chanology member ended up becoming disillusioned with the group due to their militant direction. This is what ended up starting the chain of events that ended LulzSec. Emick started a whole security company (BackTrace Security) as part of a revenge scheme for how she was hounded by Anonymous, and she eventually ended up doxing Sabu. There are many historical examples of this in members of Communist parties who became disgruntled and quit, only to be recruited by the FBI and sent back as moles.

The best time to filter out potential future informants is in the recruitment and vetting process. There are multiple reasons why someone like Sabu should never have been admitted to a serious group. His bloviating, abrasive, and braggadocious personality should have been a red flag: this person cannot shut the fuck up. Unfortunately, his bragging and social engineering skills allowed him to 'awe' younger members of Anonymous. The cult of personality that developed around Sabu was due to his ability to manipulate people, not any special technical skill. A proper vetting

procedure should prevent people like this from joining. The ideal member of a revolutionary hacking organization is stable, ideologically committed to the cause, technically competent, and also displays a sense of humility (or at least 'quiet professionalism'). Cowboys/Rockstars/Assholes need not apply. The ideal hacktivist is more like Tflow than Sabu.

People with an admitted history of for-profit criminal hacking (greed), brag a lot (ego), or are wishy-washy in their commitment are problems. Do not admit them to your organization. There is not much you can do about the fear that comes from the threat of incarceration. Quiz/Interview them on ideological issues as well as technical issues and OPSEC. You should observe people and/or get to know them for a while before you invite them. After behavioral and technical interviews/screening you can start onboarding them. If they fail at this stage, give them text files explaining general, non organization specific information on hacker OPSEC and (basic) technical skills as 'study material'. Tell them to go back, study some more and come back later with a different username.

When you onboard people you have to explain to them that revolution is not a game or an adventure. Explain the potential consequences of revolutionary hacktivist activity(such as incarceration or worse), and ask that they should agree to accept this as a possibility if they want to be part of the group. Explain that they may be asked to leave the organization at any time for security reasons and that this is not a personal slight. They must understand and accept all these conditions.

One of the main problems with informants is that the knowledge of them, and the associated paranoia, can cause tension in an organization. While security consciousness is good, paranoia is counterproductive. Understand that while moles may exist, if every member of your organization practices good technical hygiene and OPSEC discipline at all times, the risk should not be so great that it paralyzes all action.

How to spot an informant

Unfortunately, there is no tried and true way to spot an informant. A mole can be anyone: any race, gender, sexual orientation, etc. (although if you are practicing good OPSEC you should not know any of those personal details). In the world of hacktivism it can be a (formerly) trusted member of the group who has decided to cooperate with law enforcement. The best way to deal with informants is at an organizational level: that is to formally structure your organization such that there is no single central point of failure, and to practice proper compartmentation of information.

Some possible red flags [7]:

Unexplained Absence – A person who is usually active breaks their pattern of activity (ex: is offline for 24/48 hours straight when they usually spend every waking minute online). This is relative to their normal pattern of activity. They don't say anything about taking a break in advance, and when they come back they have a suspicious explanation. This person may have been arrested and turned.

Personality Shift – A member's personality suddenly changes so that they become more belligerent/militant. They may suggest operations against targets outside of the group's usual profile (ex: hey guys, lets hack the CIA, NSA, and FBI!). They may agitate for your group to do things outside your group's normal operations (ex: hey guys, lets sell drugs and malware on the dark web for extra funds!).

Fed baiting – They ask you to hack things they could have hacked themselves. They loudly encourage you to hack certain targets but don't actually personally participate (note that participation alone does not guarantee they are not an informant as there is usually leeway for an informant to commit 'acts' in the course of their informing). They provide information on target vulnerabilities out of the blue (passed on from handlers) of targets that were not on the group's radar before, and try to get the group to penetrate this otherwise random target (esp. if it is a high profile federal government agency or federal government-contractor corporation).

N.S.A. (Non-State Actor) – The person suggests the group target governments that are adversaries of the government of the nation that is investigating them (being used for 'dirty work' - plausible deniability). If they participate at all it is in these types of operations (ex: in a US/UK based hacker group, the person does not personally participate in any hacks of US/UK targets despite heavily encouraging them, and only *personally* joins in when hacking a third world nation).

Cult of Personality – An "older" or "more experienced" person joins your group or circle and soon becomes a counselor of sorts to the youngest, most edgy, most insecure, most angry, or most naive members. He "cuts them out of the herd" in order to pull them into plots. (This is a classic tactic of the agent provocateur.)

Big Spender – A previously broke hacker suddenly has tons of money to pay for stuff. If someone offers to pay money for "dox" or other de-anonymizing personal information on members of your organization (or anyone), your fed alert should be going off. What the feds lack in know-how, they can make up for with tons of cash.

Wearing a Wire – They ask you to reaffirm things (sometimes over and over) which everyone already knew or at least implicitly understood. "*Hey guys, we're all part of this big hacker conspiracy that did X, Y and Z, right?! Please sign on the dotted line so they can read the logs back in court, thanks*".

Hall Monitor – This person periodically pops in at all hours to ask about the whether or not person Y is online or not. This is to correlate online activity of a certain handle with offline activity (ex: Y leaves the house, and the informant pops in to ask "hey, is Y online?"). This is so they can build a case that hacker with alias 'Y' is in fact the person in the house.

Babbler – The person repeatedly violates, or attempts to bait others into violating common OPSEC guidelines by getting them to contaminate their identities (link them with discarded nickname(s) by calling them that in chat), talking about operational details, etc.

Histrionic – When confronted about these behaviors and/or directly questioned about being a snitch, the person becomes testy and accuses their accuser(s) of being informants. The person engages in gaslighting, guilt tripping, and

emotionally manipulative behavior, and if all else fails, becomes hysterical and irrational. This person becomes despondent at the suggestion that the group cease activities, or that certain members are planning on leaving, or that the person themselves should be 'exited' from the organization. This is because the informant still wants to collect as much information as possible on their former comrades for the lightest possible sentence. "*You're leaving like a coward? Fine, just abandon me! Leave me to rot! we've gone too far now!*"

If a person displays one of these behaviors, they may just be overeager. If they engage in two of these behaviors you should start to worry. If they engage in three or more of these behaviors, your alarm bells should start to go off.

It is possible that a person who acts this way is simply a toxic personality. There is no way to know whether or not they are actually an informant with 100% certainty. Not that it matters – the only real difference between a fed and an undisciplined person is the amount of damage they can do to your group. This person should be politely ejected from the organization. If they weren't an informant, you just got rid of a problem. If they were, you prevented them from collecting even more information and causing even more damage. This is why it is important to vet/pre-screen potential members so that if one of them suddenly starts acting this way, you know they are an informant and not just a fool.

Individual Learning

Most hackers are self-taught, and for the most part, this works. A person is far more motivated to learn hacking if they 'learn by doing' and teach themselves. However a lack of formal education can result in some gaps in fundamental knowledge. In an environment where one bad keystroke can lead to potential decades in prison, professionalism and mastery are key.

Most university lectures involve a professor reading from slides that are derived from one or more textbooks on the subject. In order to self-teach these skills, one can use youtube tutorials, 'open courses' documentation, and of course, simply experiment. However a good starting point would be to look at the curriculum of degrees in cybersecurity, information technology, information assurance, digital forensics, computer science, computer/management information systems, etc. Many universities have their curriculum for these degrees (and the syllabus for each class) publicly available. Every syllabus usually includes a textbook for the course. Through a simple google search, or a search on a torrent site, it is often the case that someone has already scanned the book and created a PDF file of it. Download these files (using a VPN of course) and read through them. Websites like 'libgen.is' also provide a variety of PDFs and e-books that you can search through.

Industrial cybersecurity and networking certifications also often have *study guides* associated with them, which again, are usually available in PDF/e-book form somewhere. Examples of these include the CompTIA line of certifications (A+, Network+, Security+, Linux+, PenTest+, CASP+, CySA+, etc.), the Cisco line of certifications (CCNA, CCNP, CCNP Security, CyberOps, etc.), and the GIAC [Global Information Assurance Certification] line of certifications, and of course the ISC2 line of certs (SSCP, OSCP, CISSP, etc.). Something like CEH (certified ethical hacker) is useful too. These are just some examples of the many cybersecurity/networking 'certifications' out there.

If you can find any PDFs/e-books of study guides for these and read through them you will be very knowledgable on these topics. Much of the material will focus on cybersecurity defense rather than offense, but it is still relevant because you have to know the other side in order to defeat it.

Of course, book learning can only go so far and eventually after learning these topics you have to get some hands on experience. There are several ways to do this. For one, there are multiple websites out there that let you hack them legally, or have 'penetration testing labs'.

An alternative to these 'legal hacking' sites is to set up your own hacking 'lab', a closed virtualized environment where you can legally practice hacking as much as you want/need. Governments and militaries sometimes refer to this type of setup as a 'Cyber Range', with the analogy being to a gun range for firearms. There are many guides, courses, and videos out there on how to set up a hacking lab as well.

Finally, there are other 'Red Swarm' manuals on many of these topics you can refer to as well.

IMPORTANT: Do not, engage in any sort of hacking or hacktivism without first mastering these technical disciplines and OPSEC. This applies both at an individual level and at an organizational level. If even *one* member of your organization is an incompetent, it could lead to them being arrested and the unraveling of your whole organization. It is better to have a smaller group of highly skilled hackers than a large group of mediocre ones, because even one bad apple is enough to spoil the bunch. *Even if you believe you are a highly technical person*, you should still use the resources outlined above to become even more competent and more skilled. There is always more to learn. No matter what their background, every new member should be subjected to a training regimen on your organization's practices, structure, general OPSEC, counterintelligence/counter-interrogation, and all manner of technical training before ever being allowed to set foot upon the open internet or interact with active cells/members. This process can be at minimum a few months (6 months recommended) and up to 2 YEARS for those who start with a relatively low level of technical knowledge. Your organization should be built to last, and you don't do that on a shaky foundation. Special attention should be given to both OPSEC and digital forensics (network forensics in particular). New members must promise upon pain of ejection from the organization, not to use their hacking skills on the open internet, under ANY CIRCUMSTANCES, *until they are fully trained*, and then only in line with the organizational goals and instructions.

Your organization should create its own curriculum, text(.txt) file sources explaining common techniques, etc. Your organization should have one or several members responsible solely for training new recruits and checking up on them frequently to see how their self-training is going, ask them questions about their progress, etc.

Organizational Learning

One of the key differences between hacker groups and the agencies that hunt them is that these agencies have decades of experience. Individual members of these agencies can have varying levels of skill, experience, and competence. However, collectively, as an organization, they continue to build on past knowledge, even as agents retire, move on, etc.

This, along with the fact that the agencies are backed by the power of the state (a monopoly on the use of force), explains part of the huge power imbalance between the two sides and the relative lack of success on the side of the hackers.

<u>There are five main goals of hacktivist organizational learning</u>

1. Developing, improving, and employing new techniques or tactics that can enable the group to change its capabilities over time.
2. Improving its members' skills in applying current techniques or tactics.
3. Collecting and utilizing the intelligence information needed to mount operations effectively.
4. Thwarting countermeasures and improve the group's chance of surviving attempts to destroy it.
5. Preserving the capabilities the group has developed even if some of its members are lost.

"A [group's] ability to learn is [the] primary determinant of [its strength], since learning is the route through which organizations can seek solutions to the problems that bound their freedom of action and limit their ability to pursue their goals in changing operational and security circumstances." [8]

For groups to be able to learn effectively, they must be willing to experiment with new techniques, tactics, and strategies. For example, when Anonymous' DOS tool, "LOIC" stopped being effective, they ended up enhancing the DDOS attacks with botnets. Leadership must be willing to gracefully accept *some* operations failures as part of the learning experience.

<u>Tradeoffs</u>

As with counter-intelligence, there is a tradeoff between centralization and decentralization in organizational learning: More centralized organizations have better 'strategic learning', long term planning and ability to coordinate large, complicated operations that involve many moving parts. On the other hand, decentralized organizations allow for greater low-level or 'tactical' innovation and higher operational tempo (they don't have to wait for central approval to start an operation).

Information Sharing

There must be sharing of technical and other information between cells and/or members of the group. This is necessary to pass on know-how on whatever techniques/tactics the group has used successfully in the past. Members/leaders of cells should write documentation (nothing that reveals operational details of past operations, of course) that functions as 'how-to' guides for other cells and future members. This can include step by step hacking guides as well as actual code (scripts, malware/exploit code, etc.). This information should be shared in a text format (.txt files) to minimize the amount of space needed, plus they have less chance for security vulnerabilities (like PDF files for example).

These documents should be shared across the organization to ensure that lessons and experience of one group are learned and retained by the organization as a whole, accelerating learning and adaption to new circumstances.

Cyberspace and Meatspace

There is a question of where, *physically*, to hack *from*. As per rule#5, you are never supposed to hack from home. This is so in the worst case scenario where you do screw up somehow, they don't trace your IP back to your house. Logically, there are only a few options. Which one you choose depends on your situation and how much money you have to blow. Note you should be using TOR at any of these places as well, or else the FBI will be showing up at the coffee shop the next day to pull the router and try to do forensics on it or something.

1. Coffee Shop or Fast Food Establishment – This is a common one, you simply go into a coffee shop (or McDonalds) which has wifi and hack from there. Obviously never use the same place twice. Downsides are the fact that there's noise, distractions, and the fact that someone could see what you're doing if they look at your screen. In all likelihood they won't know what it is, but it is a risk. Also the feds could creep up on you and grab your laptop while pretending to be random civilians, that's how they got the silk road guy. Coffee shop is better than fast food place, because at Starbucks you can pretend you're working on a startup or a novel or something if anyone asks you a question.
2. Public Library – Same pros and cons as a coffee shop except with less noise.
3. Parking Lot – If you have a car, you can use your laptop from the parking lot outside any place with free wifi. This way you don't get ID'd by an in-store camera. The downside is that if you drive, it's possible for your license plate to get ID'd on the way there by any traffic/highway cameras. If you are getting weak signal its possible to boost it with a 'cantenna', i.e. a metal can which turns a standard USB wifi device into a directional antenna and therefore extends it's range. There are tutorials for this commonly found online. If you are too lazy to make a cantenna, there are commercial 'Long Range High Speed Wi-Fi Boosters' available online. The only problem is you have to put the cantenna/wifi extender on top your roof which looks somewhat suspicious. You can use a 'Wheel desk' i.e. a tray of sorts which attaches to your steering wheel and allows you to put a laptop on it.
4. Wardriving – If you have another hacker friend in real life, you can have them drive around while you search for open or easily cracked wifi on your laptop. Then you can connect to it and use that. Obviously never use the same hacked wifi twice. The problem with this is the same as the parking lot thing, your license plate can be ID'd, if all the hacks are coming from places that your car was seen driving past it won't take a genius to put two and two together.
5. Wifi Dongle – More common in developing countries than the US. Buy a mobile hotspot/wifi dongle that has prepaid data on it. Then you can use the wifi from wherever you want, whether thats a car, secret hacker warehouse bunker, etc. Just not your house. Obviously use cash for this, and be aware that there are CCTV cameras in a lot of places that could be used to ID you when you buy it, if any hack is traced back to that device. Maybe wear a hat, use cash, and never look up or something. Buy many of these and discard them in a forensically secure manner after you use up the data.
6. F Society – If you have a whole crew of geographically co-located hackers (i.e. real life friend group), then you can hack from some abandoned squat or warehouse or something. Possibly even set up networking equipment/cantenna to share a hacked wifi connection from a nearby business. Or use the dongle idea. This is risky because you can still be geographically located if someone screws up and traces your ip back (mobile

hotspot can be triangulated). But at least it won't be your actual home address, so your people can move if you get paranoid.

7. Party Van – Combine the wardriving strategies and wifi dongle/cantenna strategies. Instead of the stationary squat, you use a Van, Minivan, Cargo Van or RV. Check out one of those tutorials on youtube on how to make the van comfy with a couch and seats and a table inside or something to put a laptop computer on. Drive around from wifi spot to wifi spot, like a hacking road trip. Maybe put a curtain or sheet in the back so when someone gets out of the van to go take a piss at Starbucks everyone in the parking lot doesn't see 2, 3 or 4+ maniacal hackers typing away on their computers in the back of a van. If you use an RV you can probably find a version of the wifi extender specifically for RV's.
8. Iceman – Rent out a hotel/motel room across from a business and hack into their wifi (or use it if open). Again, if a bunch of hacks are found coming from places that suspiciously correlated with hotel rooms your rented, it doesn't take a genius to put two and two together. This is also an extremely expensive option. But assuming you only screw up once it could be ok. Obviously, don't use the hotel's wifi where you have to authenticate with your room key or something because that links back to you.
9. From Home – If you *really* need to break rule#5 for some reason, at least don't use your home internet that your real life home address, billing information, and credit card information are attached to via your ISP. Hack your neighbor's wifi or something. If a fed TOR expert or someone shows up they can eventually determine that the TOR traffic is coming from your apartment using a directional antenna. At least the presence of other users will slow down the process slightly. I suppose if there are multiple open Wifi networks in the area you could alternately use each one. Again all of these networks are around your home /apartment so eventually they'll figure it out.

These are just some ideas, I'm sure there are others. All of these strategies rely on giving you one free pass for messing up with TOR. If your IP repeatedly gets owned there none of these strategies will save you in the long run, unless you want to live like a fugitive permanently. Always confirm and double check that you are routing all traffic through TOR before you do anything else! All it takes is one screwup, one day, and they have your IP address!

Stages of a Cyber Operation

There are several stages of a cyber operation [9]:

1. Planning: selecting the target, creating a plan, etc.
2. Preparation: gathering the necessary elements, e.g., tools, ppl, intel; rehearsals
3. Execution: conducting the operation
4. Escape and Evasion: avoiding the response from the defenders
5. Exploitation: getting value from the results of the op, e.g., money, propaganda, etc.

The exploitation phase is the most important. For hacktivists this is primarily the optics/propaganda value that comes from website defacement or information being released.

If you really want to get advanced you can "pre-script" operations i.e. simulate the operation in a virtualized environment and automate the process. The requires a quite bit of preliminary surveillance/poking around inside the target system before hand. Of course, there is always the danger that the system in question will be changed after you surveil it but before you complete the automation script. In this case you may have to start again from scratch.

Escape and evasion is also an extremely important part of the operation. Obviously exfiltrating data/etc won't be much good if you get raided by the feds and locked up the next day.

The 'ideal' hack is the one that is never discovered. Obviously if your group wants to exploit this particular hack for optics purposes (taking credit for it on social media for example), this isn't possible. But you may want to disavow certain operations. Ex: information exfil from a government contractor that exposes some of their abuses. The optics value may be great, but you might calculate that the this would attract additional attention from law enforcement that would make it not worth it. It's possible that certain penetrations will not be discovered for weeks, months, years, or even ever. In the US the statute of limitations for most hacking offenses is 5 years. So if your penetration remains undiscovered for 5 years, you're in the clear.

According to The Grucq [9],

Before a compromise time is on the attacker's side. They just need to compromise one system and they'll have access. After the compromise, time is on the defender's side. They just need to discover one single IOC (indicator of compromise) and they can roll up the compromise… Finally, the iterative cyclical nature of attack and defense means that once an attacker is discovered and purged, they can attempt to compromise the target again. This cycle results in time being an asset to alternating sides, depending on which one controls the network.

Cyber operations have multiple vectors on which to measure time:

- *Time on the compromised system (dwell time)*
- *Time from compromise to breach to – maybe – discovery*
- *Time required for exploitation of the compromise*
- *Time until the criminal liabilities expire*

Different attackers and operations are affected to a greater or lesser degree by these times depending on their purpose.

Different operations have different requirements. If you want to do long term intelligence collection you will periodically go back and exfiltrate more data in which case you have a 'long dwell time'. On the other hand, you could have a smash and grab type operation with a relatively short dwell time (hopefully minutes or less with a scripted/automated attack).

Strategy and Targets

The question of what targets to select is both an ideological and practical question. One of the main problems with clandestine revolutionary organizations is that members of the organization tend to have more radical politics than the average person and end up forming an echo chamber because their main source of social interaction is their fellow revolutionaries. This is why it is important for revolutionary hacktivists to maintain normal social ties and friendships in their 'real lives'. The process of radicalization is a slow one, and it's often only after years of frustration with reformist and less edgy forms of politics that people end up turning to radicalism. While members of the organization may already be ready for revolution, the rest of society and the general population aren't there – *yet*. The point is to choose targets that are the subject of popular outrage or at least are generally unpopular, and thereby make the revolutionary organization more popular – and also by a slow process (periodic dissemination of exfiltrated information about the abuses of the current government, agitprop on social media, etc.) to lead the 'masses' in general, gradually, to a point where the majority realize that revolution is the only solution.

There is a term for this that comes from the philosophy of the Chinese revolutionary and philosopher Mao Tse-tung: the "mass line".

<u>The Mass Line: from the masses, to the masses</u>

In the words of Mao himself [10]:

In all the practical work of our Party, all correct leadership is necessarily "from the masses, to the masses". This means: take the ideas of the masses (scattered and unsystematic ideas) and concentrate them (through study turn them into concentrated and systematic ideas), then go to the masses and propagate and explain these ideas until the masses embrace them as their own, hold fast to them and translate them into action, and test the correctness of these ideas in such action. Then once again concentrate ideas from the masses and once again go to the masses so that the ideas are persevered in and carried through. And so on, over and over again in an endless spiral, with the ideas becoming more correct, more vital and richer each time.

To link oneself with the masses, one must act in accordance with the needs and wishes of the masses. All work done for the masses must start from their needs and not from the desire of any individual, however well-intentioned. It often happens that objectively the masses need a certain change, but subjectively they are not yet conscious of the need, not yet willing or determined to make the change. In such cases, we should wait patiently. We should not make the change until, through our work, most of the masses have become conscious of the need and are willing and determined to carry it out. Otherwise we shall isolate ourselves from the masses. Unless they are conscious and willing, any kind of work that requires their participation will turn out to be a mere formality and will fail.... There are two principles here: one is the actual needs of the masses rather than what we fancy they need, and the other is the wishes of the masses, who must make up their own minds instead of our making up their minds for them.

If we tried to go on the offensive when the masses are not yet awakened, that would be adventurism. If we insisted on leading the masses to do anything against their will, we would certainly fail. If we did not advance when the masses demand advance, that would be Right opportunism.

V.O.R.D.S.: How to Select Targets

When deciding on a target of an operation, one has to weight the benefits against the costs to your organization and it's mission. While Mobley explains how media exposure both benefits the organization (by popularizing it) and also damages it (counterintelligence), a more detailed breakdown or model is needed:

- Value – The value of exfiltrated data. This can be difficult to determine in advance because what is in the data won't be known until after exfiltration. It could be nothing, or it could be a secret trove of documents that has Snowden level effects on society. It could also be financial or technical information/resources that help the organization but don't do much in terms of propaganda value. Finally, there is the hard to determine value of 'demoralizing' a hacked adversary, especially if they considered themselves security-conscious (ex: embarrassment of a 'cybersecurity' firm being hacked).
- Optics – The very act of having hacked something (particularly if accompanied by website defacement, related social media agitprop, etc.) can be a propaganda win because it excites the masses and is newsworthy. On the other hand hacking *certain* targets could damage the reputation of the organization in the eyes of the public.
- Risk – The chance that hacking a target could increase efforts by law enforcement or other actors to de-anonymize, identify, and eventually arrest members of your organization. Higher profile targets, like government agencies and corporations that work as government contractors have a very high 'risk' factor.
- Defenses – How difficult the target is to hack. Some organizations/corporations have good cyber-defenses, others don't.
- Strategic – A bit of a fudge factor. How the target fits into overall long term plans and goals of the organization. Can change over time. You can use this to account for the current mass popularity/trust of an institution, and therefore any negative blowback by the masses.

An *example* table given (you should make your own VORDS analysis since this is depends on your own assessment of the situation at any given time).

Target	Value (+)	Optics (+)	Risk (–x2)	Defenses (–)	Strategic (+)	Score
Intelligence Agency	10	9	10	10	10	-1
State Law Enforcement	9	8	6	2	5	8
Bank/Financial	9	10	5	7	10	12
Local Police	9	9	5	2	5	11
Right Wing Think Tank	10	10	3	1	10	23
Right Wing Media Org	5	8	6	2	10	9
White Supremacist Org	10	10	3	1	10	23
Government Contractor	10	10	9	8	10	4
Hospital	0	0	2	1	0	-3
Health Insurance	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Oil/Natural Gas	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Green Energy	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Trade Unions	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Airlines	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Cannabis	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Technology	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Green Energy	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Animal Agriculture	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Celebrities	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Television/Media	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Retail	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Military	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Right Wing Politicians	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Federal Government Org	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>
Senate/Congress	<etc>	<etc>	<etc>	<etc>	<etc>	<etc>

Rationale: Some categories (ex: green energy, unions) are probably bad targets because they are popular among the 'liberal' masses that need to be won over. Others (like the military) are high value but have an extreme amount of risk (also, the military is a very 'trusted' institution in society). Finally, some targets (like hospitals) have notoriously bad cybersecurity, but are also bad targets optics-wise. Any targets chosen should be chosen with helping the oppressed masses in mind, and with damaging the ruling class and it's repressive state apparatuses as much as possible, with a bias towards avoiding 'collateral damage', or accidental negative side effects on large amounts of working class people.

When you make your VORDS chart it should not be 'general industries/categories' like here, but actual individual organizations/companies, which have 'defenses' score based on your preliminary surveillance, as well as experience.

The calculation is much different for hacktivists than cyber-criminals since their objective is to monetize their exfiltrated data (ex: sell the stolen credit cards on the dark web), while if the hacktivist comes across similar personal information,

they should redact it, since their goal is not to ruin random people's finances, but to expose the truth. Furthermore the hacktivist wants to take credit for the hack to raise the media profile of the organization while the cyber-criminal wants to remain undetected for as long as possible, ideally forever.

One thing Anonymous got right was that they hacked in response to an immediate injustice. This makes the hack seem more justified as 'retaliation' when you do it (ex: company owner does something bad to their workers, you hack them in response OR a police officer does something bad to a person of color, you hack the police department in response). This is a strategy that made Anonymous popular, and it should be replicated.

Exiting the Organization

All things come to an end, even hacktivist groups. While a great deal of thought is put into recruiting people, there is less thought put into how people exit an organization. Logically, there are only a few ways it can end:

1. Quit – The member gets bored, scared, or due to real life circumstances beyond their control, can no longer make the time commitment necessary to hacktivism.
2. Arrested – The member is arrested by law enforcement.
3. Ejected – The member is ejected from the organization against their will (for behavioral or security reasons).

Your organization must have strict standardized exit procedures which ensure that minimal information is leaked when the member exits your organization. In the case that they are ejected, there is a chance that they will not follow this exit procedure but you should instruct them to follow the procedure anyway.

- Permanent Exit – All exits must be *permanent*. Once a member leaves an organization, even involuntarily due to arrest, they must be cut off from the organization forever. All information, whether chatroom passwords, server addresses, screen names, etc. That they knew must be changed over as quickly as possible to prevent exploitation of this information by the adversary. Under no circumstances can a member return to the same organization. Of course they could create a new alias and use that to infiltrate the org again, but if they contaminate that alias by linking it with their past (ejected) alias or past activities, they must be immediately ejected. A member who gets arrested should never log back on to the chat rooms/etc. after being arrested.
- Destroy all materials – The (former) member must forensically wipe all electronic devices and then *physically destroy them*. This includes USB sticks, SD cards, hard drives, computers, routers, anything capable of persistent storage of any kind. To be safe, the physical device/network card should also be destroyed.
- Forget everything – The person should try to forget any passwords, chats, aliases, etc. associated with the organization, forever.

If the member really is a mole, then they won't follow these procedures. If they are arrested they may not have enough time to follow these procedures (hopefully they have followed good security practices and encrypted all the devices they have left). At a bare minimum they should try to power down any of their devices, by unplugging them if it really comes down to it.

The Principal-Agent Dilemma

Just like with operational security and organizational learning, there is a tradeoff between centralization vs decentralization: operational control and financial efficiencies or security and organizational survival.

The [dilemma] is straightforward and nearly inescapable. To start, political and ideological leaders, or the principals, must delegate certain duties–such as planning [operations], soliciting funds, and recruiting–to agents, the middlemen, or low-level operatives. If all agents are perfectly committed to the cause at hand, agree with leaders on how best to serve the cause, and are privy to the same information as leaders about how different actions will advance the cause, then this delegation poses no problem. Under those conditions, the preferences and beliefs of the principals and their agents will be perfectly aligned, and the agents will act just as the principals would like. However, that rarely happens. Operatives' [views] almost always deviate somewhat from that of their leaders. When the preferences of leaders and agents are not completely aligned, the covert nature of [groups] necessarily implies that agents can take advantage of the situation to act as they prefer, rather than as their principals would like.

The security-control tradeoff creates a dilemma when: preferences over tactics are not perfectly aligned, so that some agents want to attack different targets or want to conduct more or fewer attacks than their leaders; principals cannot perfectly monitor their agents' tactical planning nor wield a threat of violence over them; and political goals are being placed at risk by the types of tactics operatives would employ if left to make their own decisions. All three conditions are necessary. If a group's political goals are not being put at risk, for example, then leaders have no reason to pay the security costs of exercising control.

The security-efficiency tradeoff creates a dilemma under similar conditions when: agents below the leadership are less than perfectly committed or want to spend [group resources] differently than leaders would like; principals cannot perfectly monitor their agents' uses of [group resources] nor credibly punish them for observed infractions; and resources are constrained so that leaders will not just accept the [inefficiencies] created by agency problems. Once again, all three conditions are necessary for the joint condition. If a group's resources are unconstrained, for example, then it need not care about financial efficiency.[11]

The ideal organization has no 'preference divergence' i.e. the members are perfectly aligned with the leadership's ideas on using group resources and carrying out operations. More centralized control between leadership and regular members inherently means more communications, which is a security risk. On the other hand less centralized control risks members "going off the rails" and in the context of hacktivism this means going off and hacking random targets which do not help the group's overall strategic mission. The security-efficiency tradeoff is not as relevant to hacktivist organizations because hackers are usually poor and the equipment needed is usually cheap (any computer is good for most uses).

One solution to the security-control tradeoff in hacktivism could be to create a standard "rules of engagement" text document for the whole organization that outlines, in general, what types of targets are acceptable (ex: no hospitals),

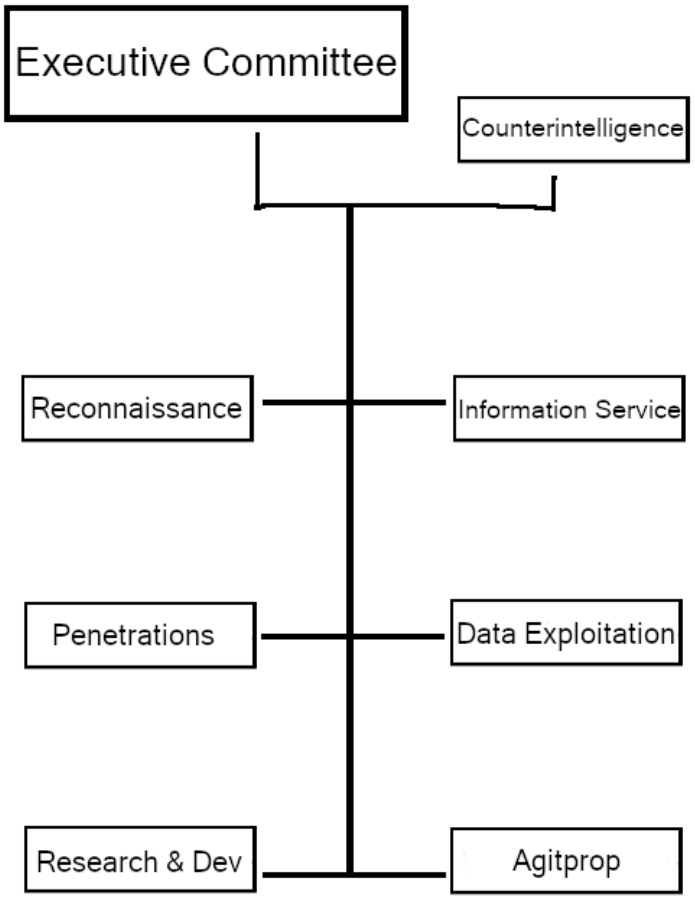
and what types of exploitation of data are permitted (ex: no personal information like credit card numbers, etc.). This would allow individual members/cells to carry out operations more independently without having to have a central leadership sign off on every single operation, causing the organization to have a lower operational tempo as a whole. On the other hand if too many cells/members are engaging in unauthorized or counterproductive activities, the central leadership could institute a policy (at least, temporarily) of having to have every operation approved. This slows things down and creates a security risk as it breaches compartmentation, but it may be necessary depending on the situation.

Organizational Structure (Proposed)

The ideal structure of a clandestine revolutionary organization is that of a highly compartmented hierarchy with subgroups for specialized roles and tasks. It should only be centralized to the extent needed to promote counterintelligence, efficiency, standardized training, organizational learning, and giving strategic direction to cells (to make sure their actions comport with larger political and/or organizational goals).

The structure of an organization also depends on it's size. A group consisting of 3-5 people doesn't really need any formal structure, whereas a group of 30 people may. An organization that has 5 people and gains an additional member should probably split the organization into 2 cells of 3 members each at that point. 3-5 members is ideal for a compartment/cell. As the organization grows, certain cells may be given certain special tasks, like intelligence/reconnaissance, penetration, data exploitation, agitprop, research & development, information sharing, internal security/counterintelligence, and leadership.

NOTE: The following is merely a proposed model and should not be taken as dogma. Any organizational structure needs to be adapted to the needs and conditions in which it operates.



Research & Development – Where you put people with a skill for coding (malware, scripts, etc.) or researching zero day vulnerabilities or other advanced/technical cybersecurity techniques. Anything they develop should be given to penetrations and/or information services for use.

Agitprop – The only part of your organization that should have access to social media. Other parts of your group should discontinue all social media and not develop individual public personas (only take credit for actions as a group). The agitprop team should come up with witty social media outreach, memes, propaganda, data dumps, etc. The agitprop team is also responsible for securely relaying this to the outside world (only connecting to social media via TOR, scrubbing EXIF/other identifying data from files and images, etc.). This is where the people who are good at theory, social media, writing, html/css, or art go.

Penetrations – The most important part of the organization since without it, the whole organization can't exist. Offensive security (black hat hackers) go here. Penetrate secure systems and exfiltrate data. Deface websites using pre-made defacement pages from agitprop, etc.

Data Exploitation & Analysis – Once you get enough data, actually reading through it and determining what is useful and what isn't is actually a full time job. Should be responsible for passing on relevant information and also redacting anything that wouldn't look good for the org if released (ex: credit card numbers).

Reconnaissance & Intelligence – Scans for targets of opportunity, vulnerabilities, footprinting, port scanning, etc. and open source intelligence. Passes on information.

Information Services – Responsible for collecting and sharing 'organizational learning' and how-to knowledge, securing the organization's systems/servers (if any), as well as training new members. IT/network pros & white hat hackers go here.

Counter-Intelligence – Have one person or a small group responsible for the human/OPSEC aspects of organizational security. In charge of rooting out moles as well as recruiting/vetting members. All paranoia about snitches should be "outsourced" to CI.

Executive Committee – Leadership that consists of 1, 3, 5, or 7 people that make a decision by vote (odd number to insure no tied votes). In charge of deciding overall strategic goals (directing penetrations on what targets are acceptable or not) and any other decisions that can't be resolved at a lower level and need to be escalated. The committee could just be made up of the leaders of the various subgroups since it's likely only needed part time and members should have regular tasks as well.

Conclusion

The left needs an explicitly anti-capitalist form of hacktivism to strike back at the repressive state apparatus, delegitimize the system, strike fear into the heart of the ruling class and its security state, and do our part to liberate the oppressed masses.

References

1. Mobley, Blake W. *Terrorism and Counter-Intelligence: How Terrorist Groups Elude Detection*. Columbia University Press, 2012.
2. Mobley, Blake William. "Terrorist Group Counterintelligence." 2008.
3. The Grugq. "OPSEC for Hackers." 2012.
4. Olson, Parmy. *We Are Anonymous: inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Back Bay Books, 2013.
5. Hewitt, Steve. Snitch!: a History of the Modern Intelligence Informer. Continuum, 2010.
6. Madinger, John. *CONFIDENTIAL INFORMANT: Law Enforcement's Most Valuable Tool*. CRC Press, 2019.
7. Wolfe, Claire. *Rats! Your Guide to Protecting Yourself against Snitches, Informers, Informants, Agents Provocateurs, Narcs, Finks, and Similar Vermin*.
8. Jackson, Brian A., and John C. Baker. *Aptitude for Destruction: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*. Vol. 1, RAND Corp., 2005.
9. The Grugq. "The 4th in the 5th: Temporal Aspects of Cyber Operations" 2017
10. "The Mass Line." *Quotations from Mao-Tse-Tung*, by Zedong Mao, Foreign Languages Press, 1967.
11. Shapiro, Jacob N. *The Terrorist's Dilemma: Managing Violent Covert Organizations*. Princeton University Press, 2015.