An Introduction to The Signs And Techniques of Online COINTELPRO

By Stephen DeVoy

Copies of this work can be purchased online at:

http://www.cafepress.com/stopfascism

Introduction

You are a political writer, an alternative journalist or just someone who knows something that others wish you did not know. You write online, perhaps on your own website, perhaps by publishing on IndyMedia or perhaps you simply post on online forums. You enjoy writing. Some readers take a liking to your style or your point of view and soon you are feeling good about your influence over the thoughts of others. It can be an enjoyable hobby. It also has a dark side.

We often make a profound mistake when we conceive of the U.S. Government as being strictly that defined by law as the official government. Government is the means by which a ruling class controls society. In the case of fascism (i.e. corporatism), the control mechanism encompasses not only the public sector, but the private sector. American society is governed by a network of moneyed interests. Included in this network are the media: television, radio and the press. The advent of the Internet has posed a challenge to the intellectual control of American society by these moneyed interests. For the first time, simple and common individuals can put forth their ideas to a large audience independent of the corporatist network. This is a major threat to the fascist state. The fascist state does not take this threat lying down. They actively seek to silence those who effectively challenge their control of information and thought.

When an individual gains notice and begins to persuade others, by means of the Internet, of a way of thinking counter to the interests of the rule class or when an individual provides information to the public that the ruling class wishes to deny the public, online COINTELPRO is tasked with silencing that individual.

Various steps are taken to identify the individual. If the individual is open about his or her identity, the task is already complete. However, if the individual posts and publishes under a pseudonym, active measures are deployed to obtain the identity of the writer. Once the writer has been identified, he or she will be cyber stalked, employers will be

contacted and a campaign of smears and disinformation will be waged with the goal of intimidating or impoverishing the writer into online silence.

The harassment will not stop so long as the writer continues publishing online. Illegal techniques are used to monitor the writer, obtain hidden information behind the material he or she publishes (e.g. IP address information not publicly displayed) and even intercept his or her email. In extreme cases, Trojan horse programs are deployed on the target's machine and used to frame the writer for illegal activities. Documents are forged in the writer's name, the goal of which is to provide evidence to a judge for the issuance of a warrant whereby all of the writer's online activities can be monitored. I know this because all of this has happened to me.

Once identified and under surveillance, should the writer expand out into the "real world," beyond the Internet, he or she will be stalked in person, harassed in person and attempts will be made to provoke his or her arrest.

This may be shocking to you. It may even be hard to believe. Nevertheless, this is exactly what happens.

I do not wish to discourage you from writing online. What I wish to do is arm you with knowledge. It is my hope that you will find ways of dealing with or ignoring the harassment – ways that are perhaps superior to my own. At the least, I wish to impart upon you what it has taken me three years to understand, thus saving you three years of your life.

To Be or Not To Be Anonymous

At first glance, anonymity appears to have strong advantages. When a person believes that she is anonymous, she will write things she would normally withhold. There is a great feeling of freedom in being faceless. Therein, however, lays the danger of anonymity. What happens, when despite your best efforts and best measures, your anonymity is lifted? Have you left a trail of things you wish you did not write? Have you revealed personal information that can be used to obtain more personal information? Will the times and dates of your posting reveal that you were playing online while at work? Will that information be sent to your employer?

Being truly anonymous, I believe, is impossible. Online anonymity requires the assumption of some degree of ignorance. You assume that those who wish to identify you do not have access to the underlying network information that could be used to identify you. Your assumptions of their ignorance can be based on your own ignorance, based upon your faith in the law and/or based on your faith in the professional ethics of others. All of these assumptions can be betrayed.

Let us begin with ignorance on your own part. You've found an online forum. You are interested in debating with the posters on that forum. You see the posts and enter their environment, trusting that you are entering a world of equals. What if you are wrong?

All forums have administrators. Being a forum administrator requires time and effort. In fact, it is a headache. Forum administrators must deal with complaints, they must comply with their host's terms of service, and they must monitor the forum. While it may be the case that some forum administrators are motivated by a love for debate, a desire to create a community, or a dedication to free speech, ask yourself a simple question; do you really believe that the percentage of people within the human population dedicated to such concerns, with ample time on their hands and sufficient knowledge of technology are large enough to support the hundreds of thousands of online forums worldwide? I doubt it. You should doubt it too.

Given this observation, it follows that one should assume just the opposite. Specifically, one should assume that a great number of forum administrators are interested in something other than a love for debate, a desire to create a community or a dedication to free speech. I propose that most online forums are a kind of Trojan horse. They are offered on false pretences. Sitting behind the forum, the administrator may be more interested in things such as making money, identity theft, blackmail, extortion and governmental monitoring. Indeed, what I have discovered is that many online forums are run by retired police officers. Several I have encountered are run by a U.S. Army PsyOps agent. Others are run by intelligence agencies.

I do not wish to make you paranoid. There are some good forums out there. I tried to run a few. When I refused to share IP information with COINTELPRO and refused to display IP information publicly, they shut me down through relentless harassment.

In my own case, the administrator of a forum on which I was posting provided all of the information he could to COINTELPRO and actively assisted them in harassing me. Given this experience, I suggest you do not use a forum unless you personally know the forum administrator.

The next level of mistake that you may make is to believe that there are no corruptible persons working for your internet service provider (ISP), web host or telephone company. The fact is that many people will do anything for money. It isn't even necessary that the amount of money offered be large. Some will do things for free if they agree with the arguments provided to them. COINTELPRO will offer cash to workers at your ISP in exchange for information. They will also tell lies about you to obtain their assistance. They may tell them that you are an anti-Semite, a pedophile, a drug dealer, a terrorist or whatever it takes to obtain cooperation. Faced with some cash and an opportunity to harm someone they believe to be evil, many people will provide the requested information.

The police will also publish material in your name to justify the issuance of a warrant. In my own case, they published an article calling for the murder of the President and another calling for citizens to shoot the police. These were forged and published in my name[1].

The average judge spends much time working with the police. There is often some kind of relationship between members of the court and the police. If an officer comes up to a judge and says, "look, I need a warrant to monitor the communications of this 'waste of life' calling on others to shoot cops," you can be sure the judge will issue the warrant, even if it is absurd that the writer would actually publish such a thing.

Once a warrant is obtained, all of your online communications may be monitored by various means, including Carnivore, a system which, ostensibly, only collects information but which I have proved elsewhere can be (and is) used to modify the packet stream leaving your machine and entering your ISP. This can be used to pretend to be you. This ability is put to evil use (e.g. framing you).

The above has led me to a counterintuitive proposal. Perhaps anonymity is not worth it? If you are never anonymous, you will write within the real social context that exists rather than some social context that does not exist, but only appears to exist due to your ignorance. If you are not really anonymous, there is no advantage to pretending that you are anonymous. You must deal with reality as it is. The reality for Americans is that we live in a fascist dictatorship and police state. Stop pretending we don't!

In order to protect yourself, you should find an employer who understands your political point of view. Do not work for someone you do not trust. If you are a writer and your employer is untrustworthy or corrupt, then he or she will act against you if and when you are singled out by COINTELPRO.

---

[1] These examples of black propaganda were assisted by Boston IndyMedia. Boston IndyMedia refused to delete these attempts to frame me. Additionally, when I corresponded with them regarding IP address access by law enforcement, they lied to me in response. There is no legitimate argument supporting Boston IndyMedia's behavior. The only rational assumption is that Boston IndyMedia is working with the U.S. Government to harass dissidents.

Signs of Online COINTELPRO

It is not always easy to know, at first, that you have been targeted. However, there are warning signs if you know what to look for. Initially, COINTELPRO deploys several personalities to interact with you. These may be multiple individuals or a single individual using multiple online names. One is often "the bad cop." He or she will argue against you and trail you as you move from forum to forum. His goal is to make sure nothing you write is posted unopposed.

Depending upon their psychological profile of you, the "bad cop" will either use argument or open hostility. Look carefully at the accusations should open hostility be used. Are they based on some knowledge of your real life? Hostility may be accompanied by outrageous accusations (e.g. that you are an anti-Semite, a pedophile, etc.). While, in all likelihood you are not what you are being accused of, think back on whether there is anything in your past that would make a cop think that these things may be true.

Police officers, more often than not, are authoritarian. Authoritarians have a very black and white vision of the world. You are either "pure" or you are "dirty." Any sexual deviance on your part may be equated with a whole slew of vile propensities in the eyes of a cop. Any criticism of Israel may be equated with anti-Semitism. Any criticism of the United States of America may make you, in his eyes, "an Anti-American piece of shit."

If you are being insulted online and vile accusations are being flung your way, look at your past from the angle of the authoritarian mind. If you can see how a semi-educated, conceptually impoverished psychopath could reach the conclusions behind the accusations, you might be the target of a COINTELPRO operation, for the police would have access to many of the odd things you may have done in your life.

Do not limit your review of your past to your adult life. COINTELPRO will contact the police department of your hometown of youth. They will obtain your school transcripts all the way back to kindergarten. If material from your childhood is being posted online or alluded to, believe me, you are a target of COINTELPRO.

As I mentioned, one of the deployed personalities is the "bad cop." This, of course, implies that there is a "good cop." Often, there are several "good cops" deployed. Some will attempt to befriend you. They will send you emails praising your beliefs and attempt to learn more about you. Be especially careful of anyone who intimates embarrassing information from "their own life" (in quotes because, they are not real people, they have no real life). This is a ploy to induce you to intimate your secrets in return.

If the harassment is becoming intense, others will offer to help you. People will come out of the woodwork and offer to assist you. When these people are people online that you do not know personally, chances are they are not trying to help you, they are trying to learn more about you or encourage you to take illegal steps against the harassers. They are just another part of the operation. In my case an FBI agent played this role. He encouraged me to do illegal things to harass my harassers, including hacking their websites. I did none of the things he suggested, and that is why I am not in prison right now.

Another thing that should alert you is anonymous email. COINTELPRO will send you anonymous email, threatening you and attempting to terrify you. Once you begin receiving such emails, block them using any filters provided with your email program. (Moreover, contact the domain of the anonymous remailer. Anonymous remailers often provide a mechanism for registering your email address as an address that does not wish to receive anonymous email. Once registered, attempts to send anonymous email to your email address from that domain will be blocked.) This is psychological warfare and it only works if you are reading the messages.

If you suspect that you are the target of COINTELPRO, go to a search engine and type in your name. Look for all instances of your name and determine whether someone is posting material using your name. COINTELPRO posts such material for a variety of reasons. One reason is defamation. They wish to smear your name. In my case they published many posts soliciting sex from children, condemning Jews and other such absurdities. The goal was to recruit others into the harassment. It worked. Another reason is to obtain a warrant to monitor you. To this end they also posted threats against government officials in my name. If you find such posts in your name, you are, more likely than not, the target of COINTELPRO.

They may go so far as to put up a blog in your name. They did this to me. They also may take articles that you have written, modify them and then repost them online[2].

There are linguistic markers used by cops as well. COINTELPRO trolls are actors. However, unlike actors you would find in a Hollywood movie, they are cops pretending to be actors. Their acting is not very good. Like most amateur actors, they will overplay their role. For example, they may try to appear to be "too hip." Online cops play games with spelling. They often will spell the word "cool" as "kewl," the word "boys" as "boyz," or the word "crew" as "krew." Since they are cops, not actual human beings, they will use cop-talk as well. Look for expressions you'd expect to see a cop writing.

Be vigilant if your personal medical information is posted. This is a sure sign that it is the government targeting you. The "PATRIOT" Act enables law enforcement to obtain your medical records. They use this information against dissidents to humiliate and harass them. In my own case, I found medical information from my early childhood posted online by cops.

[2] If your website is being spoofed in this way, keep careful track of what articles are being spoofed and the time interval between which they were copied from your website. Reviewing your logs may reveal a pattern whereby a specific IP address is used to access your website and use the copied pages for spoofing. I did this when my White Rose Journal was being spoofed and discovered that the culprit was doing this from the UCIA.GOV domain (the CIA). The spoofed website is hosted on "Beach Cities IMC", a fake IMC. The conclusion is that Beach Cities IMC is a project of the CIA.

Most cops are right wing conservatives. They carry with them a right wing interpretation of the motives and nature of a dissident. This will come out when they try to pretend to be a dissident. For example, in my case a cop opened a forum hoping to lure me to post there. He copied most of the format and choice of colors from my own forum. The name of the forum gave him away (and he later admitted that I was right about the nature of his forum). He chose the name "The Anti-American Forum." I ask you, what dissident would choose this name for a forum?

Finally, remember, you are a rare bird. Dissidents are much less common than, for example, pedophiles. The people tasked to stalk you online are trained, more often than not, to stalk pedophiles online. From the behavior of the COINTELPRO operatives that have been trailing me, I can only conclude that they have never been able to escape their initial job description. They use foul language, post links to porn websites and treat dissidents as if they are online perverts. If you are being trailed by such a dolt, you can be sure he's a cop. More likely than not, he works in the Baltimore Field Office of the FBI.

What Not To Do If You Are Targeted

First of all, do not bother filing a complaint with the FBI or your local police department. This advice applies to victims of COINTELPRO only. If you are merely the victim of a cyber stalker, then the police may be of some use. However, if you are a political writer and especially if you are an anarchist, socialist, communist, green or Muslim, it is really in your best interest to avoid the FBI and police. They will take advantage of the encounter to obtain personal information about you and file it away for future use.

Do not tell anyone that could harm you where you or your harassers are posting online. In my case, I let two coworkers know and they joined in the harassment, providing information to the harassers[3]. One of these individuals sought to take me down to advance his career. You want to avoid giving others the opportunity of cashing in on COINTELPRO payments in exchange for information. Controlling information is part of the survival process. Do not give others the opportunity to profit from the harassment you are experiencing.

Do not respond to COINTELPRO operatives. Do not reply to their emails. Do not reply to their online posts. Do not place information about them on your website, if you have one. They seek to create a feedback cycle whereby they can verify that they are having an effect on you and measure that effect. When you respond, you provide them with that feedback. The goal must be to remove the feedback.

[3] Josiah Hagen, an individual reporting to me at Cycorp, reported to the owner of the company that I was being stalked online. The owner of the company, Douglas B. Lenat, tasked Josiah Hagen with harassing me anonymously from the office thereafter. He permitted Hagen to bring an Internet appliance to work and work evenings to stalk me while I was at home in the evening. He paid Josiah Hagen to do this in the form of a bonus. The harassment that Mr. Lenat paid for included threats to my wife and daughter as well as the posting of pornography on my forum. Douglas B. Lenat himself provided me with the information I needed to reach this conclusion.

What to Do If You Are Targeted

Take down immediately from the Internet any personal information that you can. If you have websites they do not know about yet, contact your domain registrar and pay to have your websites registered anonymously.

If your employer has a website, have your company take down any references to you or your email address. Ask your company's website administrator to take the steps necessary to remove from Google's cache information from those pages where you were once listed.

Create a new email address for use in business. Use it only for business. Make sure your name is not embedded in the email address.

Change Internet Service Provider immediately. If you can, change your ISP every two months. This will make online monitoring more difficult and more expensive. It will force COINTELPRO to establish new relationships at each new ISP, consuming their time and money.

Get rid of all of your old email address and obtain new email addresses. Use a free web based email service such as Yahoo or Hotmail to create a few email addresses that you maintain only for use with new contacts. Do not give any contact a permanent email address until they've spent a long trial period communicating with you via a disposable email account. This will help you gate information about your permanent email addresses. If the temporary email address becomes a source of harassment, you can always dispose of it before giving the culprit your actual email address.

Change your telephone number and make sure the new number is unlisted. Take steps to make sure no one is entering your house or spying on you. Shred all information bearing documents that you place in your trash. Whenever possible, conduct all purchases using cash.

If you have been using a personal web-based email account from work, shut down the account and create a new one from home (not the office). Your corporation will be more than happy to cooperate with the U.S. Government in harassing you. They may already have logged the password to your private email account accessed from the office via the web.

Be cautious of anyone that just happens to come into your life. Be especially suspicious if someone new shares an amazing array of common interests with you. Guard yourself in conversation against anyone asking you highly personal questions. Warn all family members, close friends, and coworkers to not share any personal information about you with anyone whatsoever. Additionally, ask them to report to you any such requests.

If you are suspicious about some specific individual, plant unique disinformation with that person. It should be information that would be of interest to COINTELPRO. For example, tell them that you think an ex-lover is behind the harassment. Make up a name for the ex-lover and a location. Give some fake details. See if that information ends up online. If you choose to do this, make sure that only that person has the unique disinformation. If you give the unique disinformation to more than one person it is no longer unique and you cannot reliably trace it back to its source.

It's Too Late, You Are Already Deeply Entrenched

This section is for those of you that did not have the opportunity to read the first half of this pamphlet before becoming the subject of online COINTELPRO. This places you into my category: actively and deeply stalked online by COINTELPRO.

The verdict is still out on whether the harassment ever ends. I believe it will continue on some level for the rest of my life. I may choose to move to another country in order to decrease the harassment. In any case, the remainder of the pamphlet deals with the form and intent of COINTELPRO exchanges. It is broken down into several scripts. Each script briefly describes the kind of interaction that one might find on a COINTELPRO thread, where, by thread, I mean a sequence of exchanges online between the target of COINTELPRO and a COINTELPRO agent.

Before I describe these common scripts, I'd like to add that it is in your best interest to not engage in online dialogue with these people. It doesn't really matter who they are. They are paid operatives. There is no reason to figure out their identities. Your best option is to find a civil rights lawyer and sue them – not interact with them. I can not stress this more forcefully. Turn your back on them and shut them off.

Scripts

The "Who Am I?" Script

This is one of the favorite scripts used by COINTELPRO. They wish to convince you that you are being stalked by some individual that has it in for you. They will begin with information they have already collected on you. For example, by now they probably have your personnel files from previous employers, your medical records, your school transcripts and any other paperwork they can find.

Using this information, they will attempt to project a sense that they know you. Little bits of personal information will be posted online. This is bait. If you are unwise, as I once was, you will begin attempting to figure out who the harasser is. You can avoid this by coming to the correct conclusion: it's the government. However, if you choose to live in denial and avoid the belief that the government is targeting you, you just might try to "figure things out."

Figuring things out is a process of attempting to poke at a black box. You poke and watch the response. Poke and watch the response. Repeat this again and again. Each time you hope to find something out about the nature of the black box in front of you. However, as you are doing this, they are watching you. Your every attempt to poke the black box requires that you divulge more information about yourself. You mention a name. You ask a question or two. You interact with them. As you interact with them, they collect information. They collect the names you mention. They analyze your technique, your responses and your suspicions. From this information they refine their psychological model of you and then deploy this knowledge against you.

When you mention someone's name in response to their "Who am I?" game, they go off and research that person. Eventually, they refine their ability to pretend to be that individual. They have several hopes. They hope you will accuse the person. If you do,

they will send that person an email pointing out what you said and suggesting that they sue you. They'll even tell the recipient that others are suing you. I know this because I've seen the emails they send. They also hope to alienate you from the people you know and to cause you to behave as if you are paranoid. If you fall into this trap, you will become isolated and others will not believe what you write. It will be dismissed as paranoia. This is exactly what they hope to accomplish.

This script has gone so far that I have seen them post, explicitly, "Come on, who am I? Who am I? Who am I?" Their intent is obvious.

The Absurd and Outrageous Accusations Script

If you become silent and do not respond to their attempts to engage you, they often employ "The Absurd and Outrageous Accusations Script." This script is designed to compel you to interact with them. For example, in my case, they wrote an article and published it online on Boston IndyMedia. The article stated that I had been arrested in Harvard Square for offering to assist a young boy tinkle in the bathroom. Not only did this never happen, but how could one not respond to such an accusation? The accusation is so vile and horrible that any normal person would want to denounce it and declare, over and over again, that it is false and libelous. This, of course, is what they want. They want you to "end your silence and interact with them." Psychological warfare does not work unless the target is engaged. They post these libelous and defamatory articles and accusations to force you out into the open and to engage you. Once engaged, they can gather more information on you and subject you to more torment.

The most logical way, in the normal world, to refute an absurd charge or outrageous accusation is to provide a counterproof. In order to prove that the alleged event did not happen, you need to divulge information about yourself. You may need to state where you actually were when the alleged event occurred. You may need to explain just what your sexual orientation is and how such a despicable thing would not conform to your actual inclinations. As you refute their charges, they learn more about you, research it and then deploy what they learn in the form of better tuned harassment.

The best response to this script is to place a short statement, not in your name, beneath the article or message. The brief statement should read:

"The above was posted by COINTELPRO operatives. It seeks to smear and defame an activist. It is false and libelous."

That should be enough. State nothing more.

The Forged Article Script

The proper term with the intelligence community for "The Forged Article Script" is "black propaganda." COINTELPRO authors a document and uses the activist's name as the author. This technique was used against the Black nationalists during the civil rights movement in the U.S. It is used today against anarchists. The forged article is designed to attribute illegal intent, paranoia or some other defect to the dissident.[4]

This is an alternative to "The Absurd and Outrageous Accusations Script" and it is often used to "smoke you out" into the open as well. However, this form of black propaganda is actually much more dangerous. It is often used to provide probable cause before a judge. The police will allege that you did write the forged publication. If the forged publication indicates intent to engage in illegal activities or reports that you are engaged in illegal activities, a judge will consider it justification for obtaining a warrant to listen to your communications, put you under surveillance or even to invade your home.

You may be tempted to refute the article. If you do, you fall into the same trap as "The Absurd and Outrageous Accusations Script." You provide more information and they use it against you.

The best response to this script is to place a short statement, not in your name, beneath the article or message. The brief statement should read:

"The above is a forged article. It was authored and posted by COINTELPRO operatives. It seeks to smear and defame an activist. It is false and libelous. NOTE TO THE COURTS: Please investigate the law enforcement agent requesting a warrant based on the above document. It is highly likely that he authored it."

[4] Ironically, I've seen other "activists" jump on these black propaganda articles to elevate their own importance relative to a COINTELPRO target. "Activists" such as Chuck Munson, Mark Larskey, and Matt Williams fall into this category. COINTELPRO relies upon the petty nature of human beings to forward its cause and the activist community has its share of petty human beings.

That should be enough. State nothing more.

The Equivalence Script

COINTELPRO, when it is not pretending to be some individual you know, remains anonymous. They may use a name for their "krew", but that name leads no where or to a website falsely registered. Since the COINTELPRO operatives are anonymous, it does not hurt them to defame both you and themselves. When mud is flung upon multiple parties, only the known parties get dirty.

COINTELPRO operatives often pretend to be "neutral" interlopers in online discussions. In that role, they often tar both the target and COINTELPRO. They do this to sound fair and convincing. However, in the end only the non-anonymous party is harmed. That would be you and harming you is their goal. After all, they are paid to do what they do.

Since their goal is to silence you, it would serve their ends to have both you and themselves banned from a given forum or online publication. They don't really want to be there anyway. They want you to shut up. If you're not there, they have no reason to be there. In all outcomes, it is your removal they seek. They will do whatever is necessary to accomplish that goal. They have no personal interest in the forums they harass.

When you encounter "The Equivalence Script," the best thing to do is to simply note that this is what is going on. Why would any real activist take a position of neutrality in a conflict between another activist and COINTELPRO anyway? All activists should stick together. Anyone neutral in the conflict is the enemy. Make that clear and argue it strongly. Is it possible to be neutral in the matter of rape or homicide? You are the victim of a state crime. There is no room for neutrality.

Criticism from Fake Activists

COINTELPRO constantly deploys personalities pretending to be activists. If you are a target, anything you post online will be targeted with inane and pathetic criticism. Even the smallest aspect of what you write will be magnified by the fake activists. They will interpret anything and everything in the worst possible light. My advice on this is to ignore it. Real activists will see it for what it is.

Be aware that fake activists frequently use the word "we" as if they are speaking for everyone else. "Why should WE waste our time helping you?" They will post. This is a sociological device intended to provoke agreement amongst real activists. No single activist speaks for everyone else. If you see this, just point that out. Respond with, *"Don't help if you do not wish to. No one is forcing anyone to do anything."*

Finally, they will often pretend to be activists bored with your writings. This, of course, is absurd. Think about it. When you see a boring article, what do you do? If you are normal, you just don't read it and go on. You do not spend your time responding to it and elucidating to the world just how boring it is. Only a troll does that. If you are political, that troll is a COINTELPRO operative.

If you believe you must respond, just respond by writing, *"I'm sorry, the article wasn't meant for you."*

Spoofed Activists

I have witnessed, several times, the names of real activists being used in online scripts to harass another activist. When you see this, send an email to the real activist with the URL of the post where the real activist's name is used. Ask the activist if they authored the post. Chances are she didn't and will be happy to know that you asked rather than assumed that she authored the post.

The "I See You" Script

One of the primary goals of COINTELPRO is to induce paranoia. I've seen this script deployed many times. COINTELPRO will attempt to make you believe that they are watching you in real time. Don't fall for it. It is bogus.

If faced with this, you can embarrass them by calling their bluff. Ask them what you are wearing. Ask them what finger you have up at the moment. They will respond by telling you, "You are in no position to make demands of us. We call the shots!" To this, simply respond, "Well, there's your proof. You are lying, again." Leave it at that.

The "I Have Your IP" Script

Often, in an attempt to make you suspicious of the forum upon which you are posting, they will state that they have your IP address (the network address of your Internet connection). Once again, call their bluff. Demand that they post your IP address. Chances are they cannot. When they refuse, accuse them of lying.

Once you have exposed them for lying about your IP address or being able "to see" you, pound them over the head, again and again, with the fact that they are proven liars and that no one should believe anything they post.

The Paranoia Script

When evidence of black operations and other forms of harassment are exposed online and no rational means is available to discredit the information, intelligence agencies fall back on the paranoia script. The paranoia script consists of short comments characterizing the author of the evidence as "paranoid." In some cases, the intelligence trolls are explicit and make such a statement unambiguously. When they do, they add comments to the article qualifying it as "paranoid rantings" or "paranoia mongering." No argument is provided to dispute the evidence. The attack is always upon the publisher or author.

Less explicit attributions of paranoia are more common. For example, comments about "black helicopters" or "tin foil hats" are favorites of intelligence trolls. Ironically, no one on the left writes about black helicopters or tin foil hats. This reveals the cultural milieu of the intelligence troll. These insulting asides arise from rightwing culture and are common in venues such as the FreeRepublic.

Above is a photo of a black helicopter taken by the author. Upon seeing an example of the paranoia script, I decided to snap a photo of the first black helicopter I saw. The opportunity came less than 48 hours later. This should be of no surprise. Most helicopters are painted and black paint is one the options. This photo is included to show the pettiness of the black helicopter slight.

The goal of the paranoia script is obvious. Rather than refute the evidence, which often cannot be refuted, the attack relies upon discrediting the source. The left is particularly vulnerable to this kind of attack because the left practices a similar form of censorship. Political correctness has created a mindset where the value of a publication or work is directly connected to the beliefs and attitudes of author. This major defect in leftist thinking reveals a latent authoritarianism. The contents have become less important than

the authorship. This form of thinking sets up the left to be taken down through character assassination. The rightwing exploits this.

A good rule of thumb in evaluating the hidden loyalty of a self publishing website is to look for cases where those in control of the website deploy the paranoia script. This script is frequently used by members of the IndyMedia collectives in control of Boston IMC, NYC IMC, DC IMC, and Kansas City IMC. Given the history of COINTELPRO, these collectives should know better. It is highly likely that they do know better. Thus, when they employ the paranoia script, activists should interpret this as evidence of infiltration by intelligence agencies or outright ownership by intelligence agencies.

Allegations such as these are often dismissed using the paranoia script, but they are also dismissed using the "bad jacketing" script (see next script).

The Bad Jacketing Script

COINTELPRO often employs "bad jacketing" to silence and marginalize activists. To "bad jacket" someone is to accuse them of being an infiltrator or a snitch. Unfortunately, there are many infiltrators and snitches in all dissident movements. This is universally true, without regard to country or ideology. It is true in the United States as well.

A dilemma arises from this reality. If someone bad jackets another activist without cause, the act of doing so is often a good heuristic for the determination that the accuser is an infiltrator or a snitch. On the other hand, what should one do if there is ample evidence that another "activist" is an infiltrator or a snitch? The prevailing wisdom is that one should keep quiet about it unless the evidence is compelling and can be publicly demonstrated. This is often a paradox. Intelligence agents, infiltrators, and snitches are primarily drawn to information dissemination organs such as IndyMedia. From the vantage point of an IndyMedia collective, they can control the flow of information (e.g. hide posts, ban authors, allow black propaganda to be published against another activist, etc.). When confronted with this, how is the target of such an infiltrator to respond?

IndyMedia outlets, such as Boston IMC, do publish useful articles. Any IndyMedia website that is to act as an organ of COINTELPRO must preserve credibility. Maintaining credibility demands a façade of allegiance to the dissident community. This is accomplished by promoting the publications of ineffective dissidents and infiltrated organizations. The illusion of dissent remains, but it is a useless form of dissent which does not threaten the goals of the state. When an activist discovers that such an IndyMedia website is acting on behalf of the state, any public announcement of such a truth is dismissed as a form of "bad jacketing." The mediocrities that have benefited and have been promoted by the front posing as a real IndyMedia center will come to the IMC's defense. After all, their position within the activist community has been created by the IMC, a fact desirable to the state (after all, they are ineffective), and they must defend their power by defending an intelligence front, knowingly or unknowingly.

The "Security Culture" Script

Imagine the power that COINTELPRO could exert if it were to promote an activist as an expert in security culture! Such an activist would become a valued authority on who should be taken seriously by the activist community. If such an activist were working for the state, he or she could prevent more effective activists from being trusted while promoting less effective activist or, even worse, infiltrators. This is the case within the Boston anarchist community and it is likely that it is the case elsewhere.

There is great value in maintaining security against the state, whenever possible, but the fact is that unless activists drop the use of electronic communications completely, all attempts to keep information from the state will fail. The irony of this was revealed to me while a member of the BAAM (Boston Area Anarchist Movement) email group. I was a witness to a police attack on a young female activist. I had a website and was willing to write an article that would promote her cause and defend her. I made this offer on the BAAM email group only to be publicly trashed by such a "security expert." What is ironic about this is that these individuals were discussing her situation on an email group while pretending to be interested in security. If this is not a case of cognitive dissonance, then I suppose the term has no meaning.

A simple offer to assist someone can be turned down privately using one-to-one communication. Anyone who instantly jumps on such an offer and publicly trashes the offering party is either working for the state or has his own agenda, namely self promotion.

Security culture should not be ignored, but activists should not delude themselves into believing that the state is not monitoring everything anyway. If one wishes to keep the state from knowing plans or the details of some event, the entire matter should remain offline.

Conclusion

Your best defense against online COINTELPRO is to protect your online privacy but do not post anonymously unless you are willing to deal with the consequences of being identified at a future point in time. You should avoid responding to any kind of harassment. If you cannot avoid responding to the harassment, please keep in mind my suggestions about responses to the enumerated scripts. Do not engage them, dismiss them. Do not provide them with any information about your life. Force them to prove any assertions they make. Usually they will fail and you can expose them as liars.

It is a dangerous world out there. It has become much more dangerous since Bush became president. We must learn how to deal with online COINTELPRO. The best means to do this is to educate one another. I hope this pamphlet contributed in some way to that goal.