INTELLIGENCE GATHERING, DISSEMINATION, & INTERNET SECURITY

BEFORE you begin participating in any anti-fascist work, it is important to have a clear understanding of what you hope to accomplish. The purpose of the militant action undertaken by groups such as Anti-Racist Action (ARA) is to repress fascist movements/organizations and to make them incapable of operating, by means of disempowering their members, creating a culture of paranoia amongst them, and making the life of a fascist generally undesirable.

From this perspective, the goal is not to cause fascists to have a change of heart or realize the error of their ways. Convincing individual fascists to abandon their ideology isn't a bad thing, but it is not an effective focus of anti-fascist work – too much effort is put into too little outcome, and it focuses more on sympathizing with fascists rather than acting in solidarity with those they attack and oppress.

On the other hand, militantly disrupting fascist activity wherever it arises is both fun and effective!

FURTHER READING

Some of the resources listed above require a more detailed understanding in order to be used properly and securely. Listed below are a few resources where you can find a more detailed introduction to the topics.

TOR and the TOR BROWSER – Head to **torproject.org** to find instructions on installing and utilizing Tor, including the Tor Browser designed for anonymous web browsing. **Note that Tor only anonymizes your activity – *it does not encrypt it.*** This means that you should not use Tor to access your own personal information and profiles at the same time that you're doing sensitive work. An anonymous IP address doesn't mean much if someone can see that you're accessing your own Facebook profile at the same time that you're logging into your secret antifascist email account. Learn some of the details of how to properly use Tor before using it for any risky business.

OFF-THE-RECORD MESSAGING – RiseUp.net has a simple tutorial on how to set up OTR messaging using the Pidgin IM client. You can find it at **help.riseup.net/en/otr** along with a number of other tutorials on communications and tech security.

In general, **help.riseup.net/en/security** contains a lot of useful introductions to properly setting up IM and chat clients to run securely and/or anonymously.

1 Intelligence and Infiltration

SOME METHODS AND EXAMPLES

Note: Before engaging in any of these methods, familiarize yourself with proper practices regarding communication and internet security, detailed later in this pamphlet. You do not want to inadvertently give away your personal information while gathering intelligence on fascists.

1) Set up a website and/or contact email and post up fliers in neighborhoods. This not only spreads awareness of your organization, but often gets you information on local fascists.

Say, for example, you flier a Nazi's neighborhood and a concerned citizen, maybe a neighbor or former classmate of the Nazi, gives you plenty of useful information through your contact phone or email account.

You may even get Nazis contacting you who want to share information for whatever reason (they left the movement, falling out with organization, etc). This information is useful so long as it's verifiable. Either way, the person who contacted you may inadvertently give you more intelligence on him or her self (their name, phone number, or email address).

2) Set up a website for your organization. This can be a blog, a simple info page with contact info and details on local Nazis, whatever.

Someone might search Google with their name along with your organization or website to see if there is intelligence on themselves; "john smith alaska antifa". You sign into

your website and find this in the stats or referrer area (most web hosting platforms allow you to see how people found your site, including Google search terms). You run their name through the internet (try pipl.com) and find a white power Facebook profile matching the same name. You may also find a home address, phone number, etc.

pipl.com allows you to type in full names, emails, user names, or phone numbers and get deep web results (including home addresses).

3) Pretend to be a new/inexperienced Nazi, via any number of means: phone, email, Facebook, New Saxon/Aryansbook (white supremacist social network), Stormfront.org (white nationalist internet forum).

Maybe you've made a fake social networking profile on New Saxon of a young, naive, white girl interested in the white nationalist movement. Within a day you have 3 personal phone numbers and a meet up location for a private event.

Or maybe, after a few months of email correspondence and minimal phone conversation, you now hold embarrassing information on a prominent figure in the white nationalist community and have not only been invited to, but have location information on their clubhouse.

There are several other ways to gather intelligence. The white nationalist movement has internet forums and social networking sites similar to Facebook and Myspace (newsaxon.org, stormfront.org and awsnetwork.org) that you can use to your advantage. Keep your eye on the news - in Chicago, for example, there is a “mugs in the news” site and sometimes you find new Nazis, or ones you may already know about, who get arrested for hate crimes or really embarrassing and shaming crimes like pedophilia This can be exploited in obvious ways.

• TRUECRYPT
If you don't have full disk encryption enabled, Truecrypt is the next best thing. If you want to make sure no one can access your files if your computer gets seized or stolen, encrypt the sensitive stuff in a Truecrypt volume.

• ENCRYPTED EMAIL/FILES
GnuPG is a free and open source variant of PGP. Useful for encrypting email and files. You can also get a plug-in for some email clients (like Thunderbird) so that you can cryptographically sign your messages, to prove they're from you.

• FOR THE ULTRA PARANOID
TAILS on a live CD or USB. This is variant of Linux that is optimized for anonymity and security. Keep it on a CD or USB drive and plug it into any computer. Do your thing, take the CD/USB out when done. No traces. Find it at: *tails.boum.org*

• SMARTPHONES
Get an Android phone and root it. It's easier than you think. Get a modified OS, like cyanogenmod or something less off-the-shelf. Recommended Android apps:

- *Adfree*: remember, ads = malware
- *Droidwall*: firewall
- *Gibberbot*: for OTR instant messaging
- *Lookout*: antivirus
- *Orbot*: Tor
- *Orweb*: Tor-enabled browser
- *Textsecure*: encrypted text storage, also encrypts texts sent to others using Textsecure
- *Redphone*: encrypted phone calls with other Redphone users (service may be temporarily down, but will be back)
- *Whispercore*: encrypts your phone's data, among other things. Essentially hardens your phone. Unfortunately only works with some models, and like Redphone it may be temporarily unavailable.

Others that are not critical, but still worth having, especially if you prefer your online activity not to be monitored by advertisers:

- *Advertising Cookie Opt-Out*
- *Beef TACO*
- *BetterPrivacy*
- *Ghostery*
- *Google Analytics Opt-Out*
- *Optimize Google*
- *Redirect Remover*
- *Webmail Ad Blocker*
- *Web of Trust (WOT)*

• MESSAGING
Pidgin is a cross-platform IM client that works with AIM, Yahoo Messenger, Google Talk, Jabber, and others. Even better, you can get the OTR (Off-the-Record) plug-in. This will enable encryption on chats you have with anyone else using OTR. Make sure you verify who you're talking to.

• FIREWALL/ANTIVIRUS
If you're on Ubuntu, you already have Firestarter.

If you're on Windows, get one. You need it. Don't rely on the Windows defaults. There are plenty of free ones that are decent (try Comodo Internet Security). The pay ones are better; try F-Secure.

• PASSWORD PROGRAMS
Use KeePass – free, open source, good encryption, multi-platform.

Don't use Lastpass or anything that keeps your password data in the cloud.

Also recommended: Counterpane's Password Safe for Windows

2 Utilizing Your Intel

SOME METHODS AND EXAMPLES

Potential strategies and objectives: confront Nazis individually, cause rifts in their ranks, make them unable to achieve an immediate goal (demonstrations, conferences, etc), expose them to their employers and/or community, shut down their events (speaking tours, white power concerts, public social gatherings, etc).

There are many ways you can use this info. Be inventive and think about what is most practical: what will yield the best results while posing the least danger to yourself and your allies. Here are a few low-key, *very* basic examples.

1) Fliering or releasing data in a neighborhood, workplace, online etc. Fliering someone's neighborhood may result in them being confronted by people in their neighborhood, and also generally causes them to feel unsafe. Putting photos and information online can make it harder for them to get a job and easily allows co-workers, neighbors, friends and family to discover a person's white supremacist allegiances. Typically, Nazis want to hide the full details of their ideology from certain people. This method can also be done via snail mail. Try using the "address and neighbors" portion of whitepages.com, or blockshopper.com amongst others.

If you ever find or are given verifiable and juicy information on a white supremacist (they're a snitch, pedophile, etc), publicly releasing this obviously has is benefits, though every situation is unique and you should use discretion as to whether you should release their info or hold onto it for other purposes.

2) Confrontation. Instead of giving examples on how to confront someone, here are a few things to reflect on before doing so.

In a confrontation, always do your best to play it safe. Always make a serious attempt to have the benefit of 3-1 odds, numbers-wise. Serious losses on our side are very harmful to our movement and empowering to theirs. Being an antifascist, even when it comes to physical fighting, is mostly about being smart, not about being tough or honorable. We win by not only being willing and capable, but playing it smart and being tactical. When it comes to confrontation, every situation is unique.

3) Shutting down events. There are a lot of ways to shut down events – just use your head. For example, the tactics listed above can also be utilized to shut down events.

Another way to shut down an event is a phone jam (dialing an event's contact number en masse to prevent attendees from being able to receive crucial details or meeting locations).

As an example: imagine you've received an invite through your social networking account that a neo-Nazi group is speaking at a local library. You put out a statement urging people to call the library and notify them of who is speaking and let them know how fucked up it is to allow neo-Nazis to have a public speaking platform. The venue owners may be unaware of the group's identity or intentions, as sometimes fascists will book events under false names. Either way, once they find out people are pissed, this often leads to cancellations of the events. This is especially true when the venue is a place of business, as bad publicity can threaten their ability to make money.

Alternately, if the venue refuses to cancel, you could organize a protest in which a large number of antifascists block the entrance of the space and otherwise disrupt the event.

Note that Tor does not *encrypt* traffic. It can still be sniffed when the traffic leaves the exit node of the onion network.

• **BROWSER**
Firefox, latest version, with a number of add-ons. Go through the preferences to lock it down.

• **FIREFOX ADD-ONs**
Adblock Plus – Not only does this eliminate many of the ads you are normally bombarded with, it helps protect you. A lot of malware these days is delivered via ads that exploit security holes in your browser when you visit a website. These malware ads are sometimes snuck onto mainstream ad networks, so even major corporate websites sometimes carry them.

No Script – "Scripts" are little programs that your browser runs when you visit various websites. These scripts are another common attack vector for malware. If you aren't using No Script and Adblock, you can pretty much guarantee that your computer will be exploited and become part of a botnet. Now, No Script can be a little annoying to use, because a lot (most) of websites require scripts to function properly. So what you have to do is train No Script, telling it what sites are trusted and allowed to run scripts and which aren't. This can be tedious, especially at first, but it's worth it in the long run.

HTTPS Everywhere – By default, a lot of websites allow logins that are not encrypted. That means anyone who is sniffing your traffic can easily intercept this data. There are automated tools for this. You'd be amazed at what 5 minutes with one at a wifi cafe will get you. This add-on forces websites to use encryption whenever it is available, so that your traffic is less vulnerable to sniffing.

Torbutton – This will toggle Tor on and off for your browser.

4 Tech Resources

While this is designed to be an introduction to internet and computer security, some terms and concepts might be unfamiliar. You can easily find further explanation through a web search – try using DuckDuckGo.com instead of Google, if you want to avoid having your search history tracked and saved forever on Google's servers. Keep in mind that technology changes at an incredible speed, so always double-check that your information is up to date.

• OPERATING SYSTEM
Ubuntu Linux, latest version. Free, open source, and probably the most secure. Drawback is that it's less supported than other OSs (some software, graphic cards, etc. may not work on it). It's mostly easy to use, just like any other OS, but every so often to fix something you have to use the terminal to enter commands, which for non-geeks will be like filling out legal documents in a language they don't speak. There is a ton of online support on various forums, however, so it's usually not too hard to find instructions. You may want to enable full-disk encryption too (though this requires using the Alternate Installer, not the standard Ubuntu live installer).

Mac OSX is probably the runner up. If you're going to use Windows, use Windows 7.

• TOR
If you want anonymity online, you want Tor. Tor routes your internet traffic through an "onion network" so that no one can trace where it's coming from. If you're visiting Nazi websites, or otherwise don't want your online activity to be tracked, use Tor. There are plenty of tutorials and info online.

If the event won't be shut down by the venue owners, and you do not have the time or numbers to organize a blockade, staying low-key and building your intelligence can be a great option. You can watch/photograph/film from a distance and become more familiar with members' faces and vehicles, gain info on their organizational procedures, and so on.

These are just a few of the *most* simple ways to gather and utilize intelligence. There are countless other techniques and strategies for doing so – figure out what works for your circumstances.

3 Communications and Tech Security

For work involving phones, use burner phones for high-risk work (in which you might attract the attention of the state) – Google Voice or *67 can be used for low-risk work (in which you only need to hide your identity from the casual observer with no special access to your phone or internet records).

Google Voice is a way to create a phone number that appears on the caller ID of the person you are calling. It can be attached to your phone or computer and is not suggested for sensitive work. In this case, “sensitive work” is anything that could reasonably spark the interest of the state. A simple subpoena would show the accounts associated with the Google Voice.

A burner phone is a phone you buy with no contract (pay-as-you-go). You should never give your real information when purchasing one. Using a Google Voice number on your burner phone is not only unnecessary but can potentially tie your burner phone to an IP address or personalized Gmail account.

When posting sensitive internet statements (or even just for running websites, conducting web searches, and social engineering), use proxies such as Tor which anonymize your IP address. You can choose to do these activities at public wi-fi hotspots such as cafes or fast food joints, but using Tor is still preferable.

Always be safe with your email addresses. When doing antifascist work, don’t use your personal email that you use all over the internet, or your work email. Consider creating a new anonymous email account by using Tor to sign up for a free email service, and *only accessing it through Tor*.

Have good password security; random passwords with lots of characters are best (16 minimum with a mix of letters numbers).

Do not legitimately answer your the security questions. Answers for security questions should have no relevance to the actual question. For example: What was your first dogs name? Answer: Iwilldestroyeverylastoneofyou6767

Never use the same password for more than one account, or anything, for that matter.

Detailed information on tech resources and internet security can be found in the next section.