1 Chapter 2: Looking After Yourself

1.1 Coming in to help

The main work of the disinformation team is incident tracking and response. Live incidents are listed in theHive, and new ones are flagged in our slack channels as they're added. We have 5 subteams supporting this:

- Incident management
- Tech
- Outreach
- Process and training
- People

Team leads can be reached by pinging @disinfo-leads in #4-disinformation. To get involved, fill out the disinformation survey.

When in doubt, ask a team lead. Otherwise, checking social media to see if a new incident is brewing is a never-ending job.

1.2 Mental Health

Disinformation includes difficult material - it's often designed to increase emotions like fear, hatred, disgust, to form in-groups and out-groups with hate speech and images that can be difficult to view, especially if they're of a group you're part of or feel strongly about. Even those of us who've been handling this material for years still get affected (that's the point of it), so we all need to look after ourselves.

Some basics:

- Pace yourself if you're going through difficult material.
    - Take regular breaks. Don't spend more than an hour at a time reading through material.
    - If you can, arrange to be interrupted. It's easy to get into a spiral with difficult material, and find yourself hours later still digging through it. Having an alarm, or a scheduled call from a friend, or the dog pestering you for its walk etc at the end of a session can stop this happening
    - If you can, go through material with a 'buddy' - pair up with someone online, preferably with a video or audio channel, and talk through what you're doing with them.
    - Chocolate helps. We have no idea why.
    - If you start feeling wibbley, stop. There is no shame in this. Nobody in this team will ever judge you for taking a day, a week, two months off to look after yourself, or even shifting focus forever. Your mental health is important, and we will still be here when you're ready.
- If you can avoid touching or reading material, do so. That means that, where we can, we automate. If we have 50 copies of the same image, we only need to view one copy, and if it's a difficult image, not everyone on the team needs to see it.

    - If you have to share images / text in channels, put them in threads below content warnings, so people can choose whether to view them or not.
    - Automate feeds: if we have 50 copies of a message or image, only show 1 copy to the humans.
- Make disinformation something you “go to”. Right now, we’re surrounded by “the infodemic”. Friends are talking about it, feeds are everywhere, your great uncle is probably selling you the latest conspiracy theory. We’re also seeing most people in our lives online. Your life needs to include puppies and kittens, not being swamped by batshit crazy disinformation…(See Basic OpSec for our Team section above)
    - Don’t use your main social media accounts to follow disinformation. You don’t need more of that in your life. Pull the data you need using APIs; set up dedicated accounts to do the follows; ask the team if someone’s already following the accounts or groups you need data on.
    - Incognito mode. Nobody needs their ad feed full of Qanon t-shirts and bleach cures.
    - We won’t always be passive, so having some active accounts could be useful too...

1.3 Basic OpSec for our team

1.3.1 Key concepts

- Security. It’s a process. Tools help you execute the process.
- Compartmentation: separate your personal life from your work life.
- Persona: your spy disguise for research. A fleshed out human being that has details.
- Step 0: Lock your shit down.
- Goal: Impact containment. If you use compartmentation and a persona and everything goes wrong, all that gets compromised is the persona.

1.3.2 Process

OPSEC is a process, not a set of rules or tools. By continually following the process the user should remain in a state of security. The security you get is from following the process, not using tools.

1.3.2.1 Threat modeling for humans

EFF’s Surveillance Self-Defense guide has a great introduction to threat modeling. In general, think about your 1-3 biggest threats -- in our case, revealing your real identity -- and consider the following:

1. What am I protecting?
2. From whom?
    a. What are they capable of doing?
    b. What’s the worst that can happen to me?

3. How am I protecting myself and my info? (mitigate against them)

Once you've assessed your threat model, it's important to put it into action. Don't just sit there -- do it!

1.3.3 compartmentalization: Engineering to make mistakes difficult.

An important part of operational security is implementing compartmentalization to limit the damage of any one penetration or compromise. compartmentalization is the separation of information, including people and activities, into discrete cells. These cells must have no interaction, access, or knowledge of each other. This is sometimes referred to as **impact containment**.

By compartmenting your operations, the control center over your accounts, and the information available from any single persona source, you are limiting the impact of a compromise. Without proper compartmentalization, attackers are able to leverage information from one compromised account to access another related account. Increasing privileges and traversing across the persona's exposed and interlinked account control centers.

The strength of this compartmentalization is directly proportional to how strong your compartment walls are, and how well you maintain them. This takes discipline. But it isn't impossible.

1.3.4 Foundations: Personal Security

1.3.4.1 (Step 0) Baseline Security

Before you do anything else...

Secure yourself. Harden your personal environment.

- Implement unique, strong passwords everywhere
- Enable multi-factor authentication (2FA or MFA) on everything.
- Lock down privacy settings on your social media.
- Minimise your attack surface and exposure to retaliation if everything goes wrong.

Additional reading:
Security Guidelines for Congressional Campaigns
EFF's Surveillance Self-Defense Guide

1.3.5 Foundation: Work environment

1.3.5.1 Compartmentalization

No matter how good people get at hacking, they still have to obey the rules of physics.

Machines: Don't use your personal computer. Use dedicated equipment.

- At a minimum, use a Virtualbox VM.
- Better: use a separate, dedicated computer.
- Don't trust your brain to be perfect -- configure your computers differently so you have visual cues.
    - Use separate wallpapers and themes
    - Use separate browsers for separate tasks.
    - If you use dark mode on your personal computer or VM, set up light mode on your research computer or VM

Use a VPN: VPNs tunnel your internet traffic to make it look like you're in a different physical location. Use a paid product; if you're not paying a subscription for your VPN, the provider is collecting all of your traffic and selling the data.

If you're not sure which one, try ProtonVPN or Private Internet Access.

1.3.5.2 Cover: Your Persona

Once you've created your compartmented workspace, it's time to create a persona.
You're not trying to beat the NSA; you're trying to avoid being doxxed by trolls on 4chan. While it can be easy to go down a rabbit hole on this, you likely don't need a lot of backstory. With that in mind use a site like fakenamegenerator.com to create a persona.

Your persona should include at least:

- Name
- Email
- Phone number (non-VOIP burner works best if signing up for accounts)
- Account usernames and passwords
- Address
- Birthdate

Keep this info in a text file and leave it on the desktop of your working machine.

1.3.6 Work recipes (if this, then that)

Need to get people to explain the process of what they're doing, so we can build out the relevant recipes

- OSINT Research

Always start with Step 0: Baseline Security

This is intended as a quick and dirty guide to considering your Operational Security (OpSec). Consider this a starter guide or Level 0. There is a baseline for security to protect yourself, your fellow researchers, and the project. Obviously your approach to OpSec is going to depend on

your threat model. Given the current context I'm going to skip an in depth discussion of physical security in favor of other topics.

1.3.7 OpSec Appendices

The starting point for building security is to limit the potential impact of a compromise. To contain the damage from a compromise use the principle of compartmentalization. Build a strong secure compartment to use for all your work and ensure their is no taint or contamination from inside the compartment back to you.

1.3.7.1 Threat Modeling

(from Lorenzo Franceschi-Bicchierai's What is Threat Modeling?)
"The first step to online security is figuring out what you're trying to protect, and who you're up against.

To help you figure out your threat model, consider these five questions:

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those consequences?

By answering those questions, and figuring what solutions and tools you want to adopt based on them, you will come up with a threat model that works for you.

Overestimating your threat can be a problem too: if you start using obscure custom operating systems, virtual machines, or anything else technical when it's really not necessary (or you don't know how to use it), you're probably wasting your time and might be putting yourself at risk. At best, even the most simple tasks might take a while longer; in a worst-case scenario, you might be lulling yourself into a false sense of security with services and hardware that you don't need, while overlooking what actually matters to you and the actual threats you might be facing."

1.3.7.2 Physical Security Basics

- **Cover your webcam** to prevent unauthorized access to your camera.
- Lock and password protect computer
- Enable full disk encryption
- Optional: If you're concerned about unauthorized access to your microphone, you can use a mic block. Here is one example.

1.3.7.3 Passwords

Weak passwords and password recycling are the easiest ways to have your accounts pwned

- Haveibeenpwned: Check if your email account has been compromised in a data breach.

- Most password managers will alert you if your password has appeared in a data breach.

1.3.7.4 Password Managers

Password managers are the easiest way to create, store, and implement secure passwords for all your accounts.
Decision Point: Local or cloud-based password manager.

- Local: more secure, less efficient, harder to maintain, easier to lose everything if you forget to back up or lose access to your local version
- Cloud-based: easier to use, accessible anywhere, more efficient, less secure

Some options:

- 1password (cloud-based)
- LastPass (cloud-based)
- Dashlane (cloud-based)
- KeepassXC (local)

1.3.7.5 Two-Factor Authentication (2FA)

Two-Factor Authentication requires the user to provide an additional form of verification beyond just their password (Something you have + something you know). After having a strong unique password for each account, adding 2FA to an account is the highest leverage way to secure your account against unauthorized access.

- Two-Factor Authentication Handout from the EFF
- Twofactorauth.org: List of websites and whether or not they support 2FA.

Decision Point: Method for 2FA

- Text message (SMS): Easiest to get users to adopt, least secure, especially in our context. If you use it, best to use a burner VOIP number.
- Soft token (App-based): More secure than SMS. Examples include Google Authenticator and Authy.
- Hard token (Physical device): Most secure, harder to implement. Examples include Yubikey.

1.3.7.6 Using a VPN

A VPN is a program that routes all of your internet traffic through a different IP Address (like a tunnel). A VPN is one of the most effective ways to maintain anonymity online. Since VPN's basically route all your traffic like an ISP would, be sure you trust the provider. This is one of those things you should pay for, because if you're not paying for the product, you are the product. The VPN market is a racket; the review sites are a part of that. I've found thatoneprivacysite's reviews to be useful.

Here are some VPN options I've found helpful:

- ProtonVPN, by the same folks that make Protonmail

- Private Internet Access

Check that you're VPN is working properly by going to ipleak.net

Decision point: VPN on your network, on your device, or both

- On the network:
  - Pro: Filters all traffic from all devices on your network, not just web traffic or one device. If you lose VPN connection you can kill all internet access so nothing gets through without going through the VPN
  - Con: Longer and more complex setup and you need a dedicated device
- On your device:
  - Pro: Quicker and easier to get set up. Doesn't require any extra equipment.
  - Con: Only filters traffic from your one device and if it fails you may not realize immediately (unless it has a reliable killswitch). Also data your computer sends back to services on startup may get through before the VPN kicks in.

1.3.7.7 Web Browsers and Extensions

Decision Point: Which browser to use for general investigations
My browser of choice: Firefox
Essential Extensions

- Install Firefox Multi-Account Containers lets you separate your work, shopping or personal browsing without having to clear your history, log in and out, or use multiple browsers. Container tabs are like normal tabs except that the sites you visit will have access to a separate slice of the browser's storage. This means your site preferences, logged in sessions, and advertising tracking data won't carry over to the new container. Likewise, any browsing you do within the new container will not affect your logged in sessions, or tracking data of your other containers.
- Install Privacy Badger a browser add-on from the EFF that "stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web.
- Install uBlock Origin, a wide-spectrum content blocker.
- Install HTTPS Everywhere, a browser extension from the EFF that encrypts your communications with many major websites, making your browsing more secure.

1.3.7.8 Burner Email and Phone numbers (pseudonymous identities)

In the process of doing investigations, you will likely find yourself in a position where you want to create burner accounts that allow you create pseudonymous personae. When possible, I create a full identity with name, email address, VOIP phone and text as well.

- Sudo: In terms of an easy to use pseudonymous identity, I've found that sudo is a great, easy to use option. It is a paid service, so that can be a barrier, but it allows you to create a personae and associate and isolate email, phone calls, text, web browsing and payment for each persona.

1.3.7.8.1 Burner Emails

Depending on your needs you may wish to create anonymous/pseudonymous emails. These are disposable temporary email addresses you can use. Many of these will get flagged by social media services as suspicious, so it's good to know about different options.

- 33mail Free option that might get flagged
- Protonmail: Free end-to-end encrypted email
- Gmail: quick and easy commercial option that will pass muster for most services. May have issue with this if you try to sign up for a bunch with the same phone number (which you shouldn't do anyway)

1.3.7.8.2 Burner Phone and phone numbers

There are tons of ways to get a free VOIP account. One challenge with VOIP numbers is that some services you'll want to use require a real phone number and won't accept VOIP for account registration.

- Free VOIP: Google Voice. You'll obviously need an associated Google and account and getting it requires providing a real phone number (major downside).
- Paid VOIP: Burner, Hushed, CoverMe
- Burner phones: Lots of different options including Tracfone where you can get a cheap phone and swap the SIM when needed.

1.3.7.9 Secure Communications

Use End-to-End Encryption (E2EE) wherever possible. E2EE is a system of communication where all data is encrypted in transit and at rest, meaning no one (including employees at the company) has access to the data except the communicating users. This is the closest you're going to get to a completely private and secure way to communicate and store data.

1.3.7.9.1 Secure Messaging

End-to-End Encrypted messaging generally requires both users to be on the same service. This often means that the best service is the one with the most people you're trying to communicate with. Here are a few options:

- Signal is great and the How to Use Signal on iOS from the EFF is helpful. Popular among infosec, privacy enthusiasts, and journalists. One downside is that you have to tie the account to a real (non-VOIP) phone number.
- Whatsapp: Most popular E2EE messaging app. Built on the same encryption protocol as Signal. Major downside: owned by Facebook.
- iMessage: Incredibly popular. Only available to Apple users. E2EE breaks down depending on how you configure its relationship to iCloud for backing up messages.
- Others: Wire, Wickr, etc

1.3.7.9.2 Secure Email

End-to-End Encrypted email services:

- Protonmail
- Tutanota

1.3.7.9.3 Secure Ephemeral Communications:

- Firefox Send uses end-to-end encryption to keep your data secure from the moment you share to the moment your file is opened. It also offers security controls that you can set. You can choose when your file link expires, the number of downloads, and whether to add an optional password for an extra layer of security.
- CloakMy: quick, convenient and secure way to share sensitive information. Just copy your message in the box, set the recipient and your password (if you want to protect your message) and send it. The recipient will receive a secure link. If you select Auto Destruct as an expiration setting (by default), once the link is opened the message will be deleted. The message will be encrypted with a randomly generated key + your password if you chose one.

1.3.7.10 Social Engineering and Phishing

Phishing happens to everyone and it sucks. Here are a few ways to avoid getting phished.

- Urlscan.io allows even inexperienced users to investigate possibly malicious pages, such as phishing attempts or pages impersonating known brands.

A few other things to consider (which I hope we can expand upon later)

- Turn off location services on everything possible
- Locking down the setting on your social media accounts
- Removing yourself from people search sites (in case you get doxxed)
- Remove metadata from your photos before you post them
- 'This person does not exist' generates very convincing faces, again using machine learning. Reload the page to see another image. As the name suggests, these are not real people - the faces are generated entirely automatically. You can see artifacts, especially in the teeth, but this is still very close to perfect (and of course great for creating fake users).