# Advanced Security for High-Risk Individuals

# Who is a high-risk individual?

There are, for this presentation, 3 requirements to meet for being a high-risk individual:

1. Persons at genuine risk of kidnapping or serious violence
2. Threat actors are experienced at violence
3. Threat actors have a strong and genuine incentive to conduct violence

# This is NOT for:

1. Public Figures
2. Persons who don’t mind disappearing from the grid
3. Persons with Institutional support, e.g. Major journalists
4. Persons with high security budget

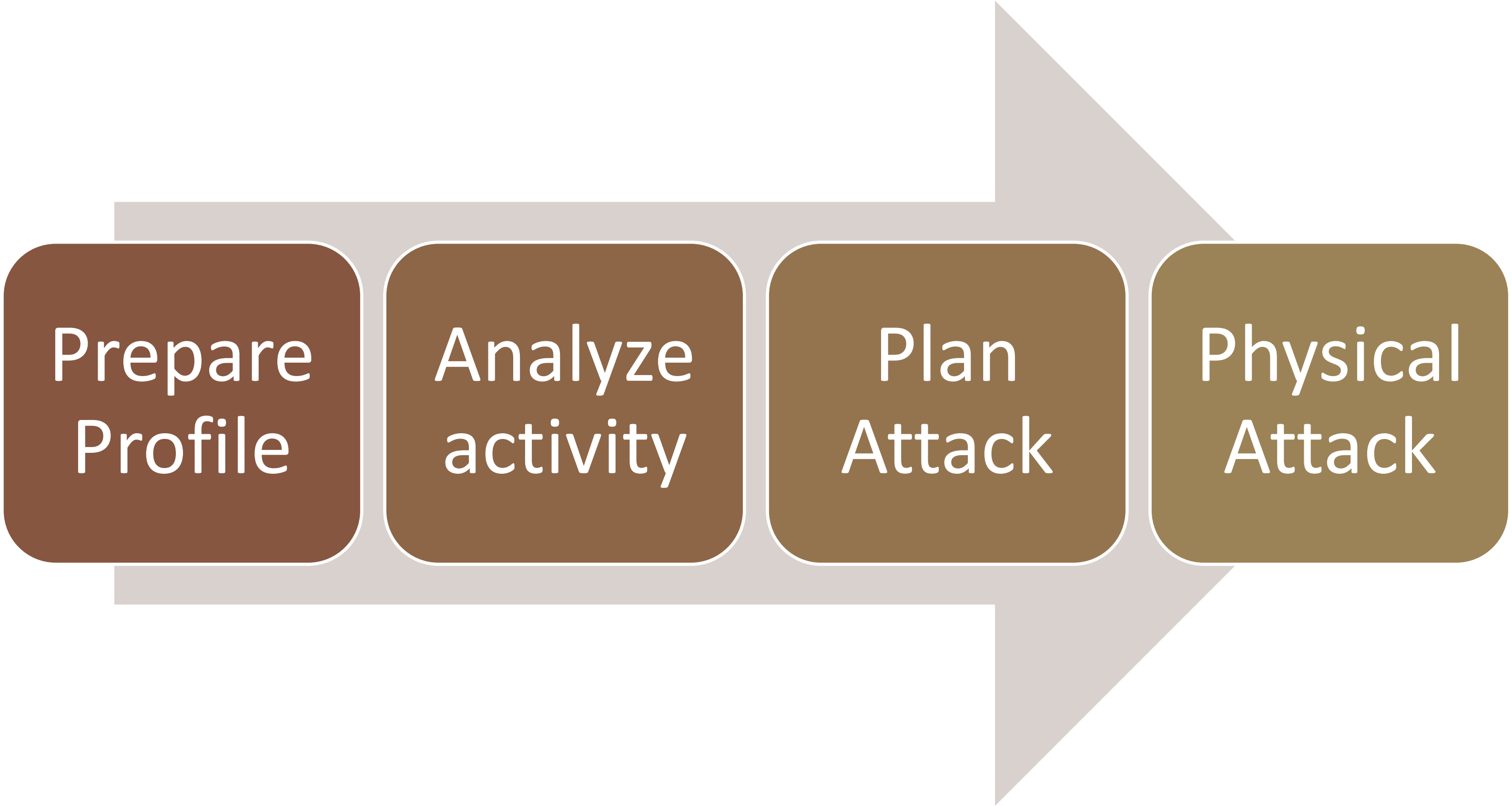
These persons would be better off referring to the gold standard of OpSec, Michael Bazzells Extreme Privacy; or even contacting experts if they can afford.

# Section 1

BASIC CONCEPTS

“WHO WILL ATTACK ME, AND HOW WILL I DEFEND MYSELF”

# Sequence of Attacks



Prepare Profile

Analyze activity

Plan Attack

Physical Attack

# Our Objective

Use Cyber Security

To Stop Chain at Activity Analysis

While We Reduce Threat

# Understanding the threat actors

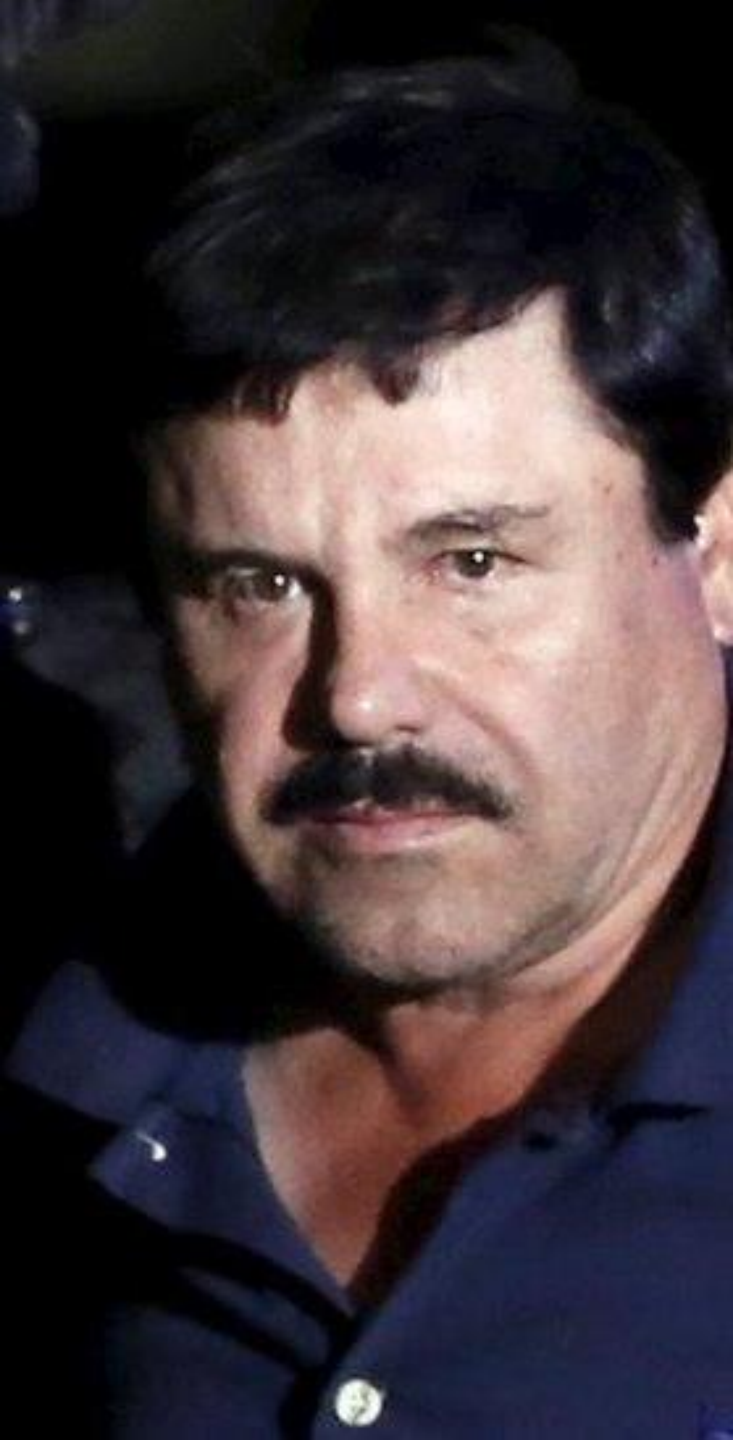
# Nation State

Countries/Warlords etc. who have lost reputation or other damages because of you; and will seek revenge. This includes high-level mercenaries.

Tactics:

1. Advanced Surveillance
2. Advanced Phishing Attacks
3. Supply Chain Attacks

The objective is usually to gather evidence and information to gauge your backing, exact data lost etc.; to fully understand the situation before ordering physical harm.



# Gangs and Cartels

Gangs, Cartels etc. have many more reasons than a genuine government to seek to harm other persons.

Tactics:

1. Doxxing
2. Spear Phishing
3. Physical surveillance

The aim of gangs and cartels is to quickly cause psychological and physical harm over targeted analysis or information gathering.

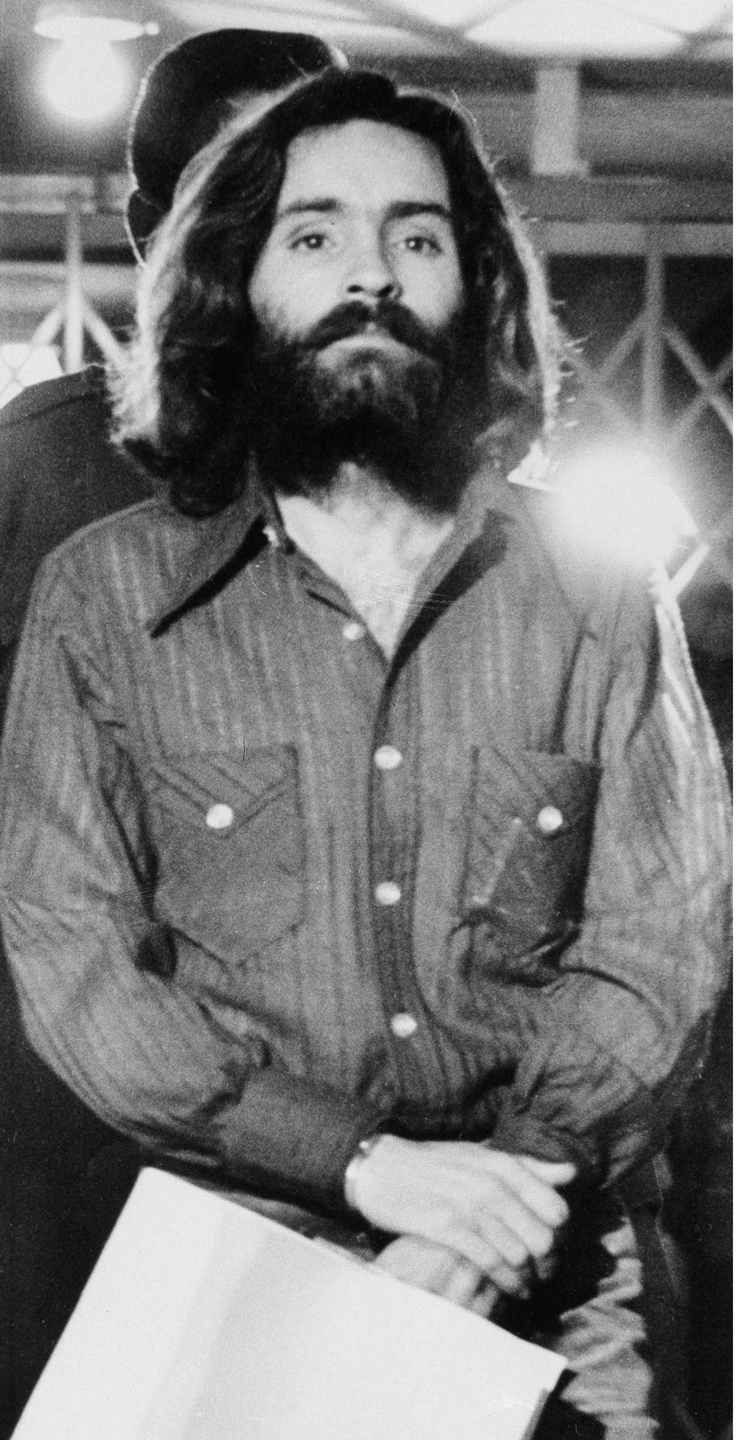
# Extremists

Extremists, who thrive on spreading fear; will obviously require to attack someone from time to time. This includes traditional extremists to online groups like incels.

Tactics:

1. OSINT Investigations
2. Social Media Infiltration
3. Social Engineering

The aim is to rapidly gain all necessary information to conduct a physical attack. They do this because they usually depend on unorganized lone actors.



# Pathological

These people are distanced from reality; having distorted views and belief systems that compel them to un-necessary, un-warranted violence. This includes everyone from habitual stalkers to ex-partners.

Tactics:

1. Stalker Ware
2. Account Takeovers
3. Social Engineering

The aim is to gain a sense of control over your behavior by gaining information over you; but can in seconds turn into a physical attack attempt.

# Reporting Isn’t Enough

These are all disconnected entities with multiple contacts

Bringing them down is extremely complex, usually taking around 3-5 years.

# Biggest Threats

Of course, if you are found; there will be undesirable results.

Hiding is extremely bad for mental health, e.g. Julian Assange

# Our objectives

Protect Location and Financial Information

Eliminating Threats (legally)

# Why Location alone?

Physical Safety is most important

Safety is key to mental health

You can’t fight due to resource asymmetry

# Evaluating Threat Level from Messaging

# Add a point for each

- Specific Details, e.g. Timeline
- Account is older than 3 months
- Calmness of tone and messages
- Detail included in threats

# Remove a point for each

Excessive swearing/filth

Humor in insults included

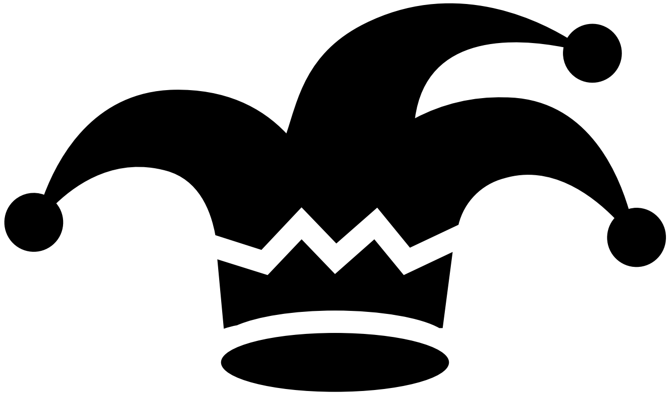
Account not older than 1 month

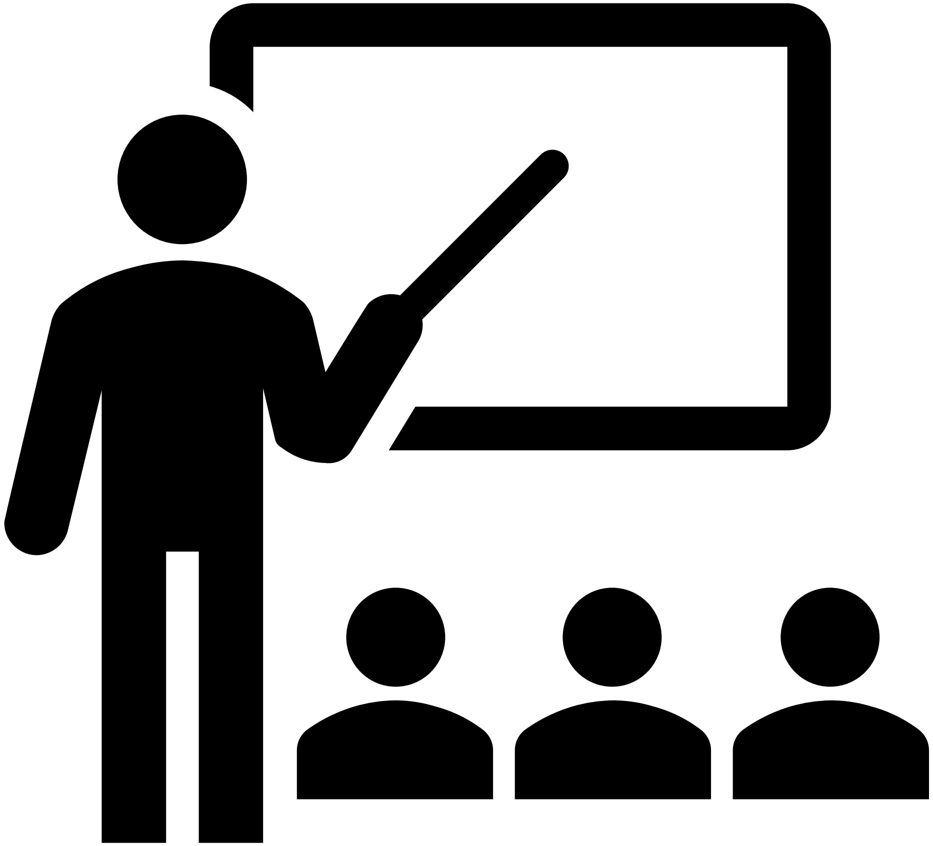
Account does not follow anyone you know

# Total points for result

IF GREATER THAN 4

IF LOWER THAN 3





# Basic Principles we use for Defence

# 3 Strategies of Data Security

Privacy

Obscurity

Deception

# Differences between

The strategies of data security:

1. Privacy means controlling access to information, e.g. Setting your social media private
2. Obscurity means making information difficult to understand, e.g. Making believable fake social media profiles.
3. Deception means **both** hiding true data **AND** providing false information, e.g. Tagging fake locations on your real account.

# Why deception works

It wastes time by keeping opponent engaged on false leads

The opponent loses heart and desire to damage with time

# 3 Types of Threat Elimination

Conventional

Asymmetric

Psychological

# Why should you engage?

Asymmetry of resources, you can’t hide forever

You should ideally be able to live a normal life afterwards

# Differences between

The types of threat elimination:

1. Conventional means traditional, physical conflict
2. Asymmetric refers to tactics that are usually referred to as “dishonorable”, e.g. blackmail, sabotage
3. Psychological refers to tactics that target the opponents’ will to fight, e.g. moral appeals, misinformation.

# Why Psychological?

Can be done with just social skills and basic resourcess

Can use it without running into legal trouble

# Section 2

## PROTECTING LOCATION

"HOW CAN THEY FIND ME, AND HOW DO I PREVENT IT"

# Vectors to find location

- Network
- Software Leaks
- OS Leaks
- OSINT

# Stage 1

1. You will hunker down into your house
2. Immediately do the following:
   1. Get credentials to a friends Amazon/similar account and log out from yours
   2. Make a list of enough supplies to last yourself 21 days
   3. Install solid barricades on doors and windows (can be easily removed from inside but not outside)
   4. Download TailsOS, GrapheneOS and Tomato and buy good amount of bitcoin

# Scrub Data

- § Backup all your most important files (including evidence of threats), **don’t touch your cloud accounts.**

- § Get your friend to send you a burner phone, 5 8GB USB drives, and a hard disk, pay friend in cash.

- § Install Tails on your computer, Graphene on your phone, and Tomato on your router.

# Scrub Data

- Get your friend to contact your ISP about setting up the connection again. Get the steps and do it; and change your name with your ISP.

- Finally, set up Murmur or Silent Phone number; and a few mail accounts with Tutanota

# Harden Devices

§On your phone: Install only Signal, Tutanota, Amazon/Similar (friend acc) and some offline games.

§On your PC: Use only built-in apps with your Tails (other than qvm/virtualbox etc)

§If needed; only use lesser known, highly reputed but open source software.

# Setting up Decoy

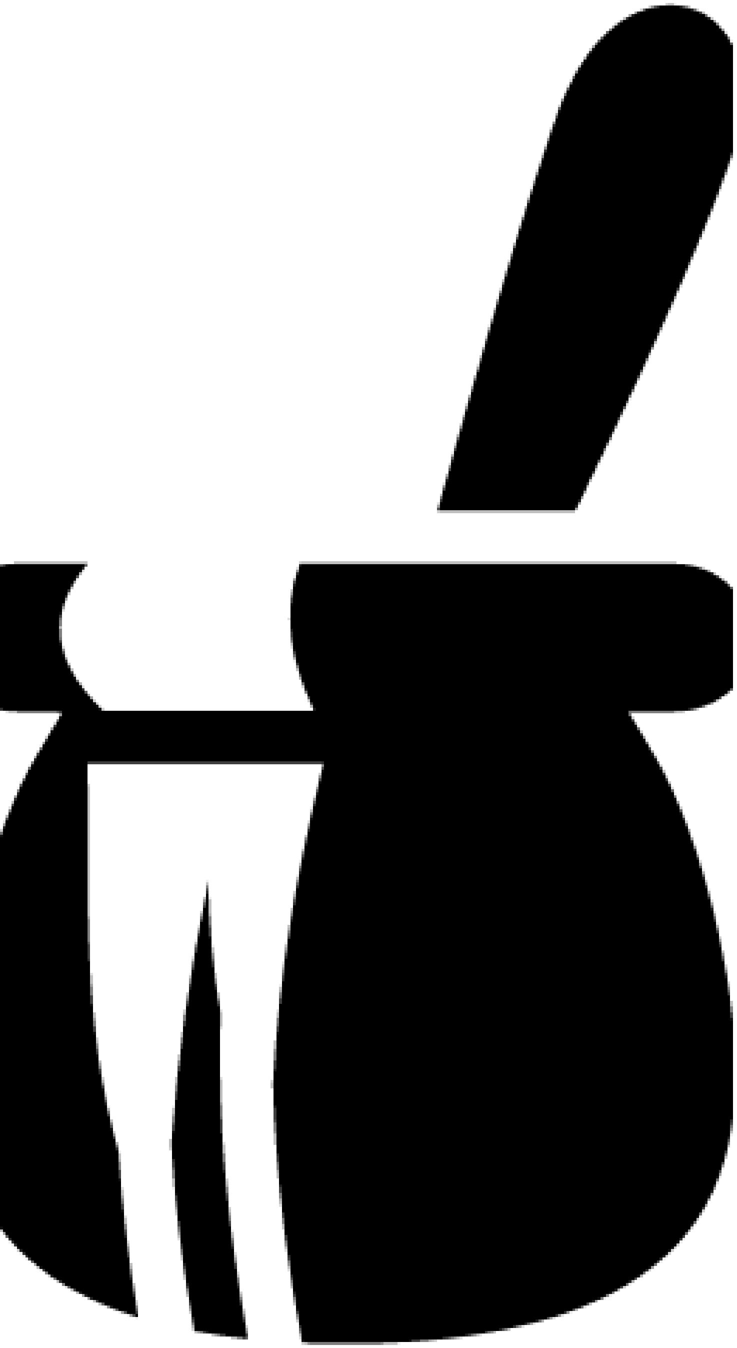
- Using Bitcoin, buy VPS (cloud machines) in 4 separate countries (think a bit before choosing).

- Set up QubesOS on all 4 of these machines.

- On the first one; set up a virtual Windows machine, and setup an automated task: Open your Gmail, twitter etc. all the big accounts.

# Setting up Decoy

- With Second VPS, set up Dropbox; and use it to upload and download files; never download or upload anything straight from your PC.
- Check for Leaks:
  - Browser Fingerprint
  - DNS
- Check for Vulnerabilities such as IoTs and shut them off.



# Using your Decoy

- On your Social Media: Regularly tweet, post stories etc. about the weather, events etc. location of the first VPS.

- Regularly plant fake evidence: Hotel bookings under your name, car rentals, pictures for social media; synchronize the timings with the time zone of the place you have chosen.

- Anything else you can do online to make it seem that you reside there.

# Using your Decoy

- Join the cheapest gym (in the area you decoy); pay with bitcoin or even your bank account, if needed.
- Leave regular yelp, google etc. reviews on local businesses, libraries etc.; based on the others left alongside.
- Regularly plant fake evidence: Hotel bookings under your name, car rentals, pictures for social media; synchronize the timings with the time zone of the place you have chosen.

# Using your Decoy

- Search pictures (and add noise) on the VPS itself, but everything else you do with the virtual machine on the VPS.

- Don’t worry about local slang etc.; you’ve apparently just shifted there. Type as you normally talk.

# Run!

§ With all the above; we have thrown off the adversaries who are certainly searching for you.

§ We can’t keep them off forever, the above is going to wear away your sanity, and fast.

§ This can only be kept up for a maximum of 15 days; after which despair will set in, you will make mistakes and leak real location.

# Run!

- Go (secretly) to a place easy to blend in:
  - If abroad, go abroad to a place like Brazil, Israel, Saudi, Georgia, Nepal; places with large expat communities and where you can blend in.
  - If domestic, go to a tier 2/tier 3 city where there is not too much surveillance with basic hygiene and safety.

# Section 3

## COUNTER-OFFENCE

“HOW CAN I BREAK THEIR MOMENTUM AND DESIRE TO HURT ME, LEGALLY”

# Warning

Due to varying legal and ethical applicability, I will list ideas without many specifics.

Also, this is potentially quite dangerous; just that to quickly move on to a normal life, this is the best bet as far as I know.

Check yourself about which of the following can be done safely and legally, and how to do them. Seek professional help at your discretion, if you want it.

# Stage 2

1. You will get a customer-facing job, first thing possible
2. This is to do the following:
    1. Restore some sense of normalcy
    2. Keep your social skills sharp, which will be essential later
    3. Keep earning money, which is always useful

# First Steps

Burn first 2 VPS

OSINT Investigation on Threat Actors

Buy new phone and HDD

Go through Digital Defence.io

# Second Steps

- Set up 3rd and 4th VPS to
- Join threat support/linked groups
- To spread rumors
- And gather personal data

# Rumour Types

You hired a scary group for protection

There is a mole within group of threat actors

The group is under official investigation by famous body

One leader said something really personal about another

A leader insulted the grass-root level persons, i.e. your gc members

And more…

# Tips for this

- Don’t just use your words, if possible
- Keep faith, word travels fast
- Don’t be shy asking for gossip after giving rumors
- Continue OSINT with new info you receive
- Change your bitcoin wallet address

# Detailed Report

After 3-6 months, compile a detailed dossier on threat actor

With all the information you have

Submit anonymously (hard + soft copy) to news and LE agencies

# After report

- You should have compiled data for 3-6 months until you submit report.

- Burn the 3rd and 4th VPS as well as your bitcoin wallet. (Transfer remainder first :D)

- Legalize the name you have been using with an affidavit, and start studying for a language exam, to move out of the country to a safe one.

# After report

- Ideally go to a country where there is absence of/widespread dislike for the community that targeted you.

- This step of studying will help you regain near complete health and sanity; just ensure to with-hold details of old life.

- Of course, once you have moved; you are quite safe.

# Last steps

At the end, after settled peacefully into new country; and having re-established contact with known persons:

- If this ordeal has exhausted you, you should look towards joining a Yoga/Zen institution; whether full or part-time.
- If this ordeal has excited you, you should look towards learning Krav Maga/Cybersecurity; and look for military/intelligence related positions.

# Last steps

These do 3 things:

1. Prevent survivor guilt/trauma from creeping up
2. Keep you fit if, god forbid, you run into future issues with anyone else
3. Increase the threat model to attack you, without increasing motivation to attack you.

# Thanks, and Regards

HOPE THIS WAS USEFUL!