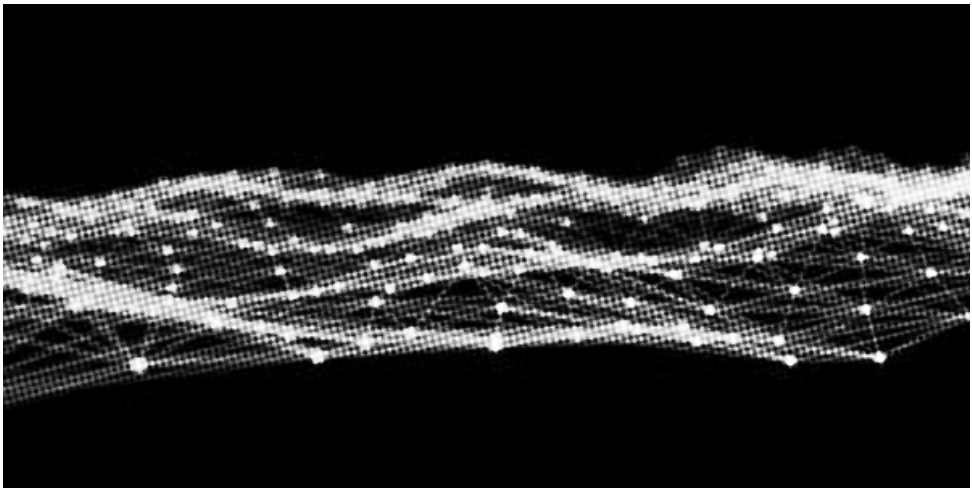
Taking Ourselves Seriously:

Digital Harm Reduction



Taking Ourselves Seriously: Digital Harm Reduction

Original text in Greek

Παιρνοντας τις εαυτους μας σοβαρα: μειωση ψηφιακων κινδυνων

2020

web.archive.org/web/20210625013117/https://radiofragmata.org/2020/11/11/pairnontas-tis-eaytoys-mas-sovara

English translation

web.archive.org/web/20210728235841/https://radiofragmata.org/2020/11/11/taking-ourselves-seriously-article-1-digital-harm-reduction

Layout

No Trace Project

notrace.how/resources/#digital-harm-reduction

Contents

Introduction

Greece is entering a new era in which the FBI, MI5, and other more advanced states in the world are acting as consultants for Greek repression. It is the responsibility of any committed revolutionary, insurrectionist, or active anarchist to adapt and grow in accordance with these developments and in the pursuit of long term struggle, and the broader preservation of our individual and collective safety.

For far too long the movement in Greece has scoffed at demands for a culture of security that is to act as a form of self-defense. Regardless of how dangerous this attitude is, it also implies a sort of hypocrisy in our approach. Do we expect our rights to be respected? Do we not take ourselves seriously? The position of the anarchist is the enemy of every nation-state, every border, and the global economy. We are choosing the most controversial and revolutionary response to this heinous society. In our choice to take a stance for true liberation, we must expect political repression without sympathy.

Without practising security culture, we hurt ourselves and communities, and help our enemies. It isn't just a matter of using this application or that, there are various procedures and approaches to everyday life we must consider in order to complicate the efforts of repression by our enemies, protect ourselves and comrades, and be successful in our projects and actions.

This article is one of a series of articles that is intent on helping to establish a broader culture of security in the anarchist movement in Greece. It is also intent on challenging certain behaviours that make the movement unsafe.

We included below some suggestions by an anonymous comrade on some basic daily ways to better secure ourselves. It is our belief that like any practice, once one is committed to it, they will grow and become more skilled in the process. Additionally we provided a translation of a text from a comrade in the USA regarding "harm reduction" and the importance of encryption and better technologies when living in the modern world.

Some Simple Suggestions for a Daily Approach to Smarter Communication and Digital Footprint

It is essential that we suggest a few consistent approaches made by revolutionaries. For one, never discuss anything formally illegal over the phone. It is true that some apps and encryption technology protect your communication greatly from State surveillance, however nothing is certain, and we must keep a healthy concern for this. This applies to writing the old-fashion way too!

It is never necessary to discuss crime or explicitly illegal acts on the phone. Be creative in your communication, but approach every conversation you write down or send on your phone by asking yourself if this could be held against you in the court of law.

Do not bring your phones to actions. If communication is necessary seek "burner" phones, and even then, try to avoid this at all cost. If there is a possibility of arrest, your phone can be the most prevalent snitch in the room.

Be careful with social media. If your identity is exposed, even with a false name, an interested enemy could find motivation to investigate if you are publishing militant political perspectives and so forth. Be careful with this, and never assume you have freedom of speech; you do in this society until the State decides you don't. Additionally, using social media such as Facebook Messenger for your source of conversation, while also posting political ideas the State may find controversial is essentially presenting an end-all portfolio of information for an investigator. Your politics are associated with your words, and those you converse are associated with your politics, and they too may be flagged as a person of interest. We must consider moving all our communication to more secure platforms such as Signal. Political or not, the State has endless funding for repressing political opponents, and a consistent approach to safe communication throughout our whole lives complicates their efforts, and helps secure a community of generally safer communication. It isn't only illegal actions that are of State interest, it is our comrades, our networks, and our broader communities.

Consider separating your emails, social media accounts, and methods of communication. Try to have separate emails for your work and political activities. Try to have separate emails for where it is necessary to have a legal identity and where it is not. Apply this also to social media. Apply this even in the case of your phone number. You can use anonymous sims to activate a Signal account or a new temporary phone number for example. You can even go so far as to change your name for certain encounters and when visiting family. All of these efforts, while deemed crazy by some, complicate State repression and surveillance.

Make sure you are deleting cookies and data on your devices when possible. Consider using VPN servers such as ProtonVPN when researching information or publishing political content.

There is no sure route to perfect security, nor do we know when the State will come knocking on our doors, and for which reason they will choose to do so. But if we challenge ourselves, and each other to maintain a decent standard of security against the State, we will be adapting and growing constantly in a direction of consistent self-defense from the never ending assault by the State. This advice is not only for the classic guerilla or fugitive, it is for everyone, and far simpler to practice and maintain than any time in history. In the USA publishers and writers alone have faced prison time, in Spain the anarchist identity itself has been criminalized, and in light of the recent Golden Dawn verdict in Greece, the New Democracy regime is likely to apply new measures to criminalize anarchists claiming they are just being fair.

As they criminalize gatherings for example, imagine the trajectory of this judicial route. What is next? Maybe investigations into “conspiracies” to gather. Giving felonies for those accused of organizing events where a riot happened to take place, solely for a call-out on Facebook or Twitter. These instances of prosecution already take place in the USA, and some individuals have done years in jail as a result of it. These types of small practices can help to deter the State's success in pursuing such charges.

There is a long term commitment in living a more secure political lifestyle. But we should not approach this as all or nothing. It is annoying, inconvenient (like all struggles), and maybe at times seems unnecessary; until it isn't.

An Argument For Digital Harm Reduction in the Movement

A specter is haunting the intelligence services of the world, the specter of the Internet "going dark". It's a concept brought up frequently as a doomsday scenario in the near future in which investigations are no longer possible and criminals get away with all their crimes because encryption has become so ubiquitous that no readable data is obtainable by law enforcement, whether legally or illegally, it just isn't available to them anymore.

This is largely a fantasy meant to scare conservative Americans, but it has truth to it and they wouldn't be telling this tale and fighting encryption so hard if it wasn't a real threat to them. In many ways we live in interesting times. One expression of that is a low level conflict over privacy between the tech world and law enforcement. They should be natural allies and they are in so many other ways but on the issue of encryption they couldn't be further apart. All the security experts agree (including those within governments), encryption is only effective if it is total. There can be no secret backdoors, no special passwords that allow cops to get in with a warrant. This would undermine the entire security model. There's consensus this special backdoor would get revealed to the wrong parties (criminals, enemy governments, etc.) and thus a contradiction has been created: in order for encryption to work for everyone, including State actors, it must make surveillance by those very State actors more difficult or in some circumstances nearly impossible.

Encryption has existed in various forms for years. The technology that allows for encrypted phone calls has existed since at least the 1980's. But these systems were expensive, complicated, and actually less secure than the free solutions available to us today. They easily cost thousands of dollars to install and you could only contact other parties who have also invested thousands in their own setup. Obviously, it was only used by those in the upper echelons of power: CEOs of major corporations and high-ranking politicians. But then the Internet happened. Affordable computers happened. Smartphones happened. And while this confluence of technologies have unleashed many horrors on the world and made it easier for the State to track our movements, it has also enabled contradic-

tions, such as accessible and easy to use military-grade encryption on a mass scale. The modern Internet era has created mass surveillance like the world has never known before, but also has provided a forum for various communication at the expense of State interests.

More and more we see investigations being hampered by encryption, but more importantly and more effectively we see a hampering of mass surveillance which makes it harder to determine who to do more intensive targeted surveillance against. This is mass encryption's greatest strength, hiding the "bad actors" within the larger crowd, making the very first step of investigations more difficult and labor intensive. And there are certain things that in the long term may become extinct or have to entirely reinvent themselves: the wiretap, or the police raid and seizure of incriminating evidence. As more of our lives move online and onto our devices, the choices we make about how to use those devices have a huge impact on the enemy's ability to repress us.

Don't believe enemy propaganda about how encryption is pointless and broken, how the State is always more powerful than our ability to protect ourselves from it, about how you should just give up. In regard to this issue, they're running scared and don't quite know what to do so they're largely using misinformation to overstate their abilities. Some companies recognize this and see economic opportunity and that's all that's going on when you see another article about a government paying millions of dollars for new Internet surveillance equipment. You're seeing scared fools being conned out of money by security industry hucksters.

Yes, they have some tricks up their sleeve. Yes, the solutions we're generally describing are not perfect, there are flaws. But we're not advocating or saying that perfection is possible. It would be better from a security perspective if we didn't use any of these technologies and lived off the grid. But that is not the case or possible for most of us. We live in the modern world and must use these devices to survive it. What we're advocating is harm reduction. The term "harm reduction" is often used in the context of safer drug and sexual practices: clean needles and condoms. Sure, the doctor says, it would be better to not use drugs and if you never had sex, you'd never get a sexually transmitted disease. But if you're going to do these

things anyways, you should reduce the possibility of harm by changing a few practices.

Digital harm reduction is what we need. A few simple practices being done differently can have a big impact. It means, for example[1]:

1. Using Signal for your calls and text messages instead of… anything else (normal calls, normal SMS, Viber, WhatsApp). Signal is the safest and easiest to use encrypted communication app available and it was built by anarchists.
2. Encrypt your computer with a good passphrase.
3. Encrypt your phone with a good passphrase.
4. Use a free encrypted e-mail solution like Protonmail for… everything.
5. Don't sync anything to the cloud or backup anything using your phone's online backup service. Typically what's backed up isn't encrypted, even if your phone is. You can safely backup your phone manually to your encrypted computer and this is easy to do, even if it's a bit more annoying.

What's a good passphrase? A series of words which are randomly selected that are easy to remember and hard to guess. Examples of good passphrases:

- orderly likely english distance melody
- column maryland possible burning happened weight

Put the spaces in your passphrase. Spaces are "free" in that they add extra length to the passphrase without making it any more difficult to remember. Length is more important than complexity so these example passphrases are much more secure than "ifgiityj993", for example. In selecting these words, use a random word generator or turn to random pages in a dictionary. Don't use your brain. It's not random. Your brain will tell you to look around the room and out the window and choose a very unrandom passphrase like "chair desk window cloud".

---

[1] *No Trace Project note:* For other, more detailed recommendations, see Digital best practices[2].

[2] https://notrace.how/threat-library/mitigations/digital-best-practices.html

Power off your devices when possible. If your device is encrypted with a good passphrase and off, you're very protected. If the device is on, there are more potential opportunities for attacking it. Try to make a habit of fully shutting down (not simply sleeping) your computer when you leave the house or when you're asleep. If your device is encrypted with a good passphrase and you believe it may be seized very soon, try to prioritize turning it off completely. This will greatly increase the protection of your data. Just to reiterate, if your device isn't encrypted, this will do nothing to help you, nothing will help you.

As a cautionary tale, we can look to the story of the black bloc that was kettled for many hours in Washington DC during the inauguration of Donald Trump several years ago. Over a hundred people were standing outside for hours, trapped by police together, essentially waiting to be arrested. During these many hours, people used their phones to talk with friends and post on Twitter and so for a while there was a bit of a live conversation and series of updates coming out of this trapped group online. During this entire time, nobody in the group seemed to have the good sense or knowledge to tell others to encrypt their phone with a good passphrase if they hadn't already done so. Moreover, none of the thousands of people online watching this situation live thought to do so either. Reports from the kettle indicated the little advice being passed around was completely unhelpful, such as people with unencrypted phones with mere "screen unlock patterns" (useless against the police) being told to turn off their phones before being arrested to "clear the memory" of the unlock pattern which supposedly (wrongly) gave greater security.

In the end at least half of the people present had their phones successfully broken into by the police and had sensitive messages and contacts compromised. Notably, the biggest similarity between most of the phones not successfully broken into was they were iPhones. The iPhone encrypts by default so when you set up your phone it forces you to choose a password, no matter how shitty, and then uses that password to encrypt the phone. On Android, at least at the time, it was not encrypted by default and you had to do it intentionally in the settings. So on this point, Apple was actually a greater ally to these comrades than anyone else. Given how poor the security practices were in this crowd, we're confident the iPhone users had

very weak passwords, probably a 4-digit number in most cases. And yet, in that situation, this was surprisingly enough to keep the cops out, who also did such a poor job at trying to break into these phones that even the most bare minimum effort was enough to protect these comrades, which makes the fact that so many comrades failed to do this all the more tragic.

Some of this naïveté can be blamed on the youth and inexperience of many present. However there were also comrades present with over 15 years experience as anarchists who acted no better. In the case of the thousands of supporters who failed to give any useful advice, there's really no excuses left and really we're all responsible as a movement for our cultural practices around digital security not being good enough.

So let's not fall into the same traps as other comrades have and do these simple practices that can greatly reduce harm to our movement. Yes, there's a lot more that can be done and this is not an exhaustive guide to living like Edward Snowden. You can always do more, but the realistic goal cannot be for every comrade to have the expertise of a computer hacker, but to try to get everyone to meet a minimum standard that can help protect us all.

This article is one of a series of articles that intents on helping to establish a broader culture of security in the anarchist movement in Greece. It also intents on challenging certain behaviours that make the movement unsafe.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention—be careful about what zines you print and where you store them.