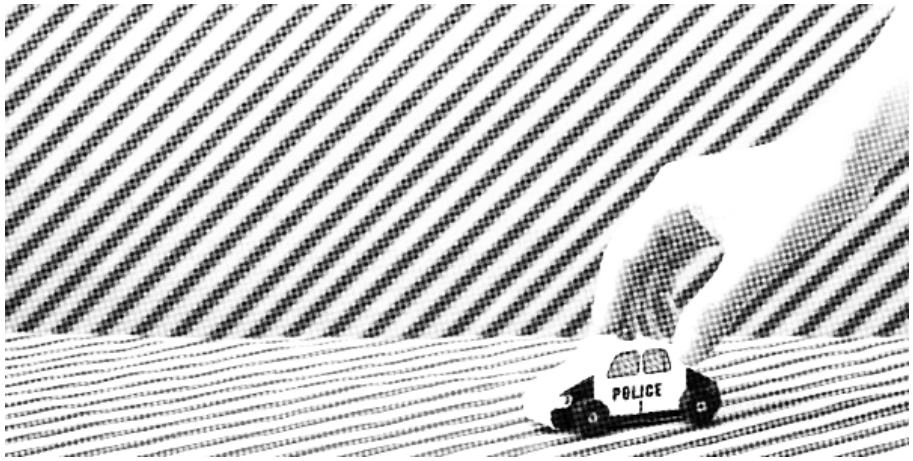
There are many guides out there that describe everything from the best ways of building timed incendiary devices, to dealing with DNA, to anti-forensic methods and how to secure digital information against search and seizure or government surveillance. Some of them are over forty years old, others are newer, some of them still hold up while others need updating. We thought it wouldn't hurt to have some suggestions, a brief “things to consider” article, that is reasonably up-to-date in regards to the enemy's methods.

To (try to) keep the cops at bay



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.

To (try to) keep the cops at bay

Original text in Swedish

Att (försöka) hålla snuten på avstånd

2020

web.archive.org/web/20201117135555/
https://325.nostate.net/2020/09/16/svart-mane-black-moon-pdf

Translation and layout

No Trace Project

notrace.how/resources/#keep-at-bay

point you probably already have a keylogger installed. To reduce the risk of this: use Linux, never open unknown emails and be aware of what you download on your computer

- During a search, unplug/shut off all electronic devices with hard drives, memory cards or network cards

There are plenty of in-depth texts on the subject, so this is just to be considered a small post-it note.

Finally, we just want to emphasize that our goal is not to make it as difficult, advanced, boring or demanding as possible to act, to physically attack the world that denies us our freedom. Each situation requires its own analysis, methods and experiments, where our proposals may be completely irrelevant. At the same time, we have learned from generations of struggle what the enemy has in its arsenal and have tried to see beyond it. We try to learn from our own and other comrades' mistakes, but equally from our own and other comrades' successes.

On the one hand: what is possible despite the intensive surveillance and forensic capabilities? On the other hand, what are the gaps where they have not yet succeeded in developing or testing their repressive methods? We fight out of desire and longing, we must want to challenge ourselves and their repression, otherwise there is no point in fighting. The enemy cannot be everywhere all the time. The shadows belong to us.

There are many guides out there that describe everything from the best ways of building timed incendiary devices, to dealing with DNA, to anti-forensic methods and how to secure digital information against search and seizure or government surveillance. Some of them are over forty years old, others are newer, some of them still hold up while others need updating. We thought it wouldn't hurt to have some suggestions, a brief "things to consider" article, that is reasonably up-to-date in regards to the enemy's methods. Some lessons and experiences combined with technical info but in a format that hopefully doesn't feel too rigid and authoritarian.

Sometimes it feels like there is a particularly repressive climate in the world or the region you live in but historically there is rarely more repression in one era than there is in another. The simple explanation is that the state is constantly waging war against its enemies, it is only more evident if one is affected by it directly or indirectly, as an individual, group or entire society. The exceptions may be situations such as world wars, but even then the mechanisms are different, and in our view it is usually possible to say that repression is constant. That is to say, it is not possible to think: I will be unaffected. Because sooner or later the spotlight will turn from yesterday's enemy to you.

We mention this because, at the time of writing, there are not many anarchists of "our generation" in "our region", broadly speaking, who have been struck by repression. We are a generation that has

been able to act relatively painlessly in bold attacks on the state while getting away with it, often without even having to consider the boundaries of nation-states or, in some cases, technological and digital developments. What we mean is not that people have been shit at security, but rather that there has been a good security culture among comrades based on non-digital methods. This has been accompanied by the development of electronic infrastructure for, for instance, publications and for obscuring who is hanging out with whom behind encrypted communications (even though, of course, the communications never contain anything that reveals criminal activity).

This generation has shared methods with each other and been successful in their respective contexts, but in the last few years there have been several occasions where comrades have been arrested or been forced to go underground, where these methods have been exposed and the security procedures have been seen through. This calls for everyone's attention. So we need to discuss, share experiences and consider how to outmaneuver the cops, when for the moment they seem to have outmaneuvered us. In some cases, it's because comrades have been careless about security by not taking precautions to avoid being watched, perhaps just because it's been so easy for all these years and the security procedures ultimately felt redundant. In very few other cases, it's thanks to cops who can think outside the box. Either way, their repressive success has given them insight into how we work.

shit incessantly. Sometimes we slip up, but one thing we never slip up on is this: we never communicate digitally about anything we don't want to tell a cop or prosecutor directly. It doesn't matter if it's encrypted; not with PGP, not through Signal, Telegram or OTR, not even in drafts of secret email addresses. We don't use smartphones, not in private, not when we take action. It is possible to use Signal on a computer, for example, but if we do, it is to hide our social contacts, not to conspire.

In our view, the basis for saving yourself and your comrades a lot of trouble, in everyday life as well as during a search warrant, is to organise your digital life like this (or similarly):

- A computer for private matters: web browsing, emailing, watching movies, etc. Preferably on an encrypted Linux system.
- A computer with persistent TAILS for contacting comrades, for projects, for possible information gathering and editing or authoring of texts, images, etc.
- If action claims are to be written: have an additional computer without a network interface, and use it with Tails to write. Never publish from a computer or network that can be connected to you
- If you have external hard drives: encrypt with Veracrypt or with Linux encryption options
- If the state manages to get into your system, with malware etc., encryption and other security measures will help little to none, as by that

vices in one of the their bicycles. Several surveillance operations against the comrade and his immediate surroundings are suggested, without revealing whether it is via an installed camera in the home, through a surveillance team or otherwise. The country's security police is responsible for conducting the investigation, so lots of information is lacking in detail.

Let's linger on the bike. This form of surveillance, secretly placing and installing a GPS tracking device in the bike's cavities, is carried out in a context where it is already part of the security procedures to search private bikes in order to avoid this particular scenario, especially in order not to attract cops to meetings or reconnaissance rounds. Unless it was the case that the comrade was careless, using his own bike without searching it—we cannot know for now, as the comrade is still trapped in the enemy's concrete cage—it may be the case that the cops have access to poorly concealed technology. Most likely, however, the comrade did not steal or borrow a bicycle and did not detach the handlebars and saddle to search the cavities with a lamp, fingers, and other appropriate tools. The lesson? Never use your own bike in an attack or anything to do with an attack on the enemy. Search the bike at regular intervals, but especially before an action, to see if extra security measures are necessary.

The authors of this text are among those who long for the death of the Internet, along with civilization and all the infrastructure that enables its survival and expansion. At the same time, we use the

Their investigations, in turn, give us some insight into how they work these days, and that's where we think we can build on to mend the security practices we've built up over generations and eras.

Nor is it just a question of technical routines, it's also about attitudes: to each other, to the world, to the enemy and to oneself. Let's take a quote from a recent manual as our starting point:

- Don't be efficient by society's standards; performing a task as efficiently as possible but then feeling like crap, treating others badly or not being able to cope for the rest of your life. None of this is much different from paid work except that you are your own enslaving employer.
- The means and the end are rarely identical; they are more like the relationship between dreams and waking life. If the goal is “no one is free until everyone is free”, then we can only try to act as freely, considerately, carefully and responsibly as possible. There will always be conflicts, conflicting emotions and incomprehensible impulses too. But if you dream of a world without social hierarchies and institutions, it's a good idea not to reproduce them in your relationships. Try to build relationships so that you can talk about any experience you share, to reduce the need to talk to outsiders about it. The more limited the conversations between you are, the more likely it is that one of you will feel the need to talk about compromising subjects to other friends

or, in the worst case, to a psychologist or the police. It's not easy, but if we're soft to each other, it's easier to be hard towards the enemy.

- NO MOBILE PHONES OR ELECTRONIC DEVICES!!! It's not an exaggeration: you're carrying a little snitch in your pocket. Leave it at home: at meetings, when scouting locations, when shopping for materials and when carrying out the action. Modern cars should be avoided and definitely rental cars, which are all equipped with GPS. If you plan to steal tools, equipment or vehicles from businesses or individuals, be aware that many have GPS transmitters on them. Try to memorise as much as you can in your head and anything you feel compelled to write down should be burned as soon as possible.

If you can avoid it, do not use the internet to gather information. There are plenty of libraries and government agencies you can visit to gather information anonymously. If you still feel compelled to use the internet, read up on and use anonymization projects like Tails, Tor, etc. And in that case, only use the internet for information gathering, never for communication about any plans. The internet is controlled by corporations and states, not libertarian hackers, even though it may be presented this way in some digital spaces.

- Leave as few traces as possible. Protective suits, face masks, gloves, shoe covers, goggles, disposable clothing (in second-hand containers or burned), anything to avoid leaving DNA at the site of the fire, construction site, crime scene or on the way there and back. Bottles and other materials left at the scene should be cleaned with, for example, Mr. Muscle gel, which dissolves grease and hair. Other comrades use sterilising agents used in healthcare or food handling but we have no experience of this ourselves.
- Know where the cameras are and avoid them. They can be found in many public places; public transport, shops, businesses, ATMs, toll booths, etc. Look for camera-free roads. If this is not possible, dress in a way that you cannot be recognised from the camera angle. Steal bikes or borrow them from distant friends and acquaintances, never use your own for an action. (Search bikes for GPS equipment). Always buy materials in cash before an action. Everything from tickets to emergency supplies, clothing and incendiary device materials. Look for safe "building sites" where you can build the incendiary devices without leaving or collecting tracks. If there aren't any, get cheap tents and pitch them where you feel safe. Then throw the tent away or burn it. Think through all the steps before, during and after the action, again and again, and consider if you could leave traces anywhere or risk being exposed later.

In a case against several comrades, the investigation shows that the cops used GPS tracking de-