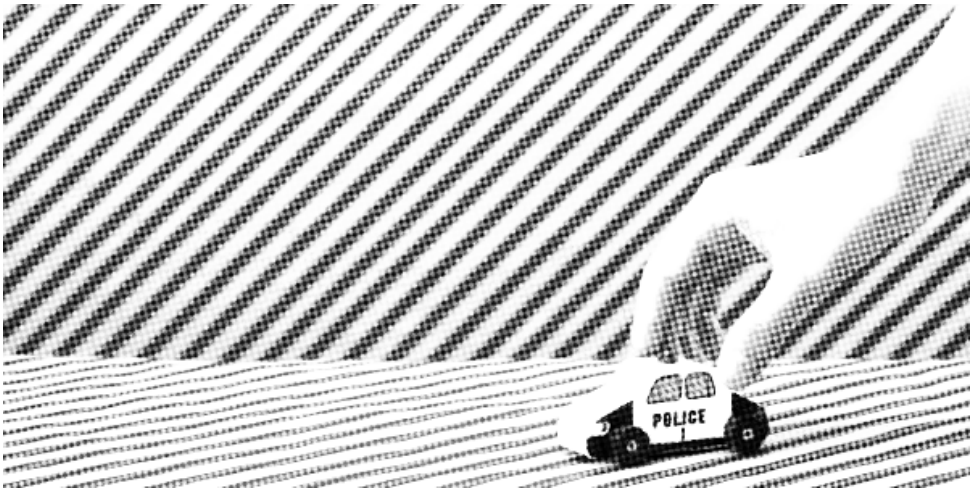
Pour (essayer de) tenir les flics à distance



Pour (essayer de) tenir les flics à distance

Texte d'origine en suédois

Att (försöka) hålla snuten på avstånd

2020

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

Traduction et mise en page

No Trace Project

notrace.how/resources/fr/#tenir-a-distance

Il existe de nombreux guides qui décrivent toutes sortes de choses, depuis les meilleurs moyens de fabriquer des engins incendiaires à retardement à la gestion des traces ADN, en passant par les techniques pour contrer la police scientifique et les manières de protéger des données numériques face aux perquisitions, aux saisies ou à la surveillance gouvernementale. Certains d'entre eux ont plus de quarante ans, d'autres sont plus récents, certains sont encore valables, d'autres doivent être mis à jour. Nous avons pensé que ça ne ferait pas de mal de rassembler quelques suggestions, un article pas trop long avec des « trucs à prendre en considération », qui soit raisonnablement en phase avec les méthodes de l'ennemi. Quelques leçons et expériences mélangées à des informations techniques, mais dans un format qui, nous l'espérons, ne soit pas trop rigide et autoritaire.

On a parfois l'impression qu'il y a un climat particulièrement répressif dans le monde ou dans la région où l'on vit, mais historiquement, il y a rarement plus de répression à une époque qu'à une autre. L'explication simple est que l'État fait constamment la guerre à ses ennemi·e·s, ce qui n'est que plus évident si l'on est affecté·e directement ou indirectement, en tant qu'individu, groupe ou société entière. Les exceptions peuvent être des situations telles que les guerres mondiales, mais même dans ce cas, les mécanismes sont différents et, selon nous, il est généralement possible de dire que la répression est constante. En d'autres termes, il n'est pas possible de penser : cela ne m'affectera pas. Car tôt ou tard, les projecteurs seront braqués sur vous et non plus sur l'ennemi d'hier.

Nous mentionnons cela parce que, à l'heure où nous écrivons ces lignes, il n'y a pas beaucoup d'anarchistes de « notre génération » dans « notre région », au sens large, qui ont été frappé·e·s par la répression. Nous sommes une génération qui a été capable d'agir de manière relativement facile dans des attaques audacieuses contre l'État sans se faire attraper, souvent sans même avoir à considérer les frontières des États-nations ou, dans certains cas, les développements technologiques et numériques. Ce qu'on veut dire, ce n'est pas que les gens ont été nul·le·s en matière de sécurité, mais plutôt qu'il y a eu parmi les camarades une bonne culture de la sécurité basée sur des méthodes non numériques. Cela s'est accompagné du développement de l'infrastructure électronique pour, par exemple, les publications et pour dissimuler qui traîne avec qui derrière des communications chif-

frées (même si, bien sûr, les communications ne contiennent jamais rien qui révèle une activité criminelle).

Au sein de cette génération, les un·e·s et les autres se sont échangé des techniques et ont eu du succès dans leurs contextes respectifs, mais au cours des dernières années, en plusieurs occasions des camarades ont été arrêté·e·s ou contraint·e·s à la clandestinité, ces techniques ont été révélées et les procédures de sécurité ont été dévoilées. Cela requiert l'attention de tout le monde. Nous devons donc discuter, partager nos expériences et réfléchir à la manière de déjouer les flics, lorsque pour le moment ils semblent nous avoir déjoué·e·s. Dans certains cas, c'est parce que les camarades ont été négligent·e·s en matière de sécurité en ne prenant pas de précautions pour éviter d'être surveillé·e·s, peut-être parce que c'était si facile pendant toutes ces années et que les procédures de sécurité ont fini par sembler superflues. Dans quelques rares autres cas, c'est grâce aux flics qui ont su faire preuve d'imagination. Dans tous les cas, leurs succès répressifs leur ont permis de comprendre comment nous travaillons. Leurs enquêtes, à leur tour, nous donnent une idée de la façon dont ils travaillent aujourd'hui, et c'est là-dessus que nous pensons pouvoir nous appuyer pour améliorer les pratiques de sécurité que nous avons mises en place au fil des générations et des époques.

Il ne s'agit pas juste de bonnes habitudes techniques, mais également d'attitudes : envers les autres, envers le monde, envers l'ennemi et envers soi-même. Prenons comme point de départ une citation d'un manuel récent :

- Ne soyez pas efficace selon les normes de la société ; effectuer une tâche aussi efficacement que possible, mais ensuite se sentir comme une merde, maltraiter les autres ou ne pas être capable de s'en sortir pour le reste de sa vie. Rien de tout cela n'est très différent du travail rémunéré, sauf que vous êtes votre propre employeur asservissant.
- Les moyens et la fin sont rarement identiques ; ils ressemblent davantage à la relation entre les rêves et la vie éveillée. Si l'objectif est « personne n'est libre tant que tout le monde n'est pas libre », alors nous ne pouvons qu'essayer d'agir de la manière la plus libre, réfléchie, attentionnée et responsable possible. Il y aura toujours des conflits, des émotions contradictoires et des impulsions incompréhensibles. Mais si vous rêvez d'un monde sans hiérarchies sociales ni institu-

tions, il est bon de ne pas les reproduire dans vos relations. Essayez de construire des relations qui vous permettent de parler de toute expérience que vous partagez, afin de réduire le besoin d'en parler à des personnes extérieures. Plus les conversations entre vous sont limitées, plus il est probable que l'un·e d'entre vous éprouve le besoin de parler de sujets compromettants à d'autres ami·e·s ou, dans le pire des cas, à un psychologue ou à la police. Ce n'est pas facile, mais si nous sommes douces les un·e·s envers les autres, il est plus facile d'être dur envers l'ennemi.

- PAS DE TÉLÉPHONES PORTABLES NI D'APPAREILS ÉLECTRONIQUES !!! Ce n'est pas une exagération : vous avez un petit mouchard dans votre poche. Laissez-le à la maison : lors des réunions, lors des repérages, lors des achats de matériel et lors de la réalisation de l'action. Les voitures modernes sont à éviter et surtout les voitures de location, qui sont toutes équipées de GPS. Si vous envisagez de voler des outils, du matériel ou des véhicules dans des entreprises ou chez des particuliers, sachez que beaucoup sont équipés d'émetteurs GPS. Essayez de mémoriser le plus possible dans votre tête et tout ce que vous vous sentez obligé de noter, il vaut mieux le brûler dès que possible.

Dans la mesure du possible, n'utilisez pas Internet pour recueillir des informations. Il existe de nombreuses bibliothèques et agences gouvernementales que vous pouvez visiter pour recueillir des informations de manière anonyme. Si vous vous sentez tout de même obligé d'utiliser Internet, renseignez-vous sur les projets d'anonymisation comme Tails, Tor, etc, et utilisez-les. Et dans ce cas, n'utilisez Internet que pour recueillir des informations, jamais pour communiquer sur un quelconque projet. Internet est contrôlé par les entreprises et les États, pas par des hackers libertaires, même si c'est parfois présenté comme ça dans certains espaces numériques.

- Laissez le moins de traces possible. Combinaisons de protection, masques, gants, de quoi couvrir les chaussures, lunettes de protection, vêtements jetables (à jeter dans des contenants de seconde main ou à brûler), tout ce qui peut éviter de laisser de l'ADN sur le lieu de l'incendie, du chantier, de la scène de crime ou sur le trajet aller-retour.

Les bouteilles et autres matériaux laissés sur les lieux doivent être nettoyés avec, par exemple, le nettoyant Mr Muscle, qui dissout les graisses et les cheveux. D'autres camarades utilisent des agents stérilisants employés par les industries de la santé ou de l'agro-alimentaire, mais nous n'avons pas nous-même d'expérience en la matière.

- Sachez où se trouvent les caméras et évitez-les. Il y en a dans de nombreux lieux publics : transports publics, magasins, entreprises, distributeurs de billets, péages, etc. Cherchez des routes sans caméras. Si cela n'est pas possible, habillez-vous de manière à ne pas être reconnu sous l'angle de la caméra. Volez des vélos ou empruntez-les à des amis et connaissances éloignées, n'utilisez jamais le vôtre pour une action. (Inspectez les vélos pour y chercher des dispositifs GPS). Payez toujours le matériel en espèces avant une action. Tout, des tickets de transports publics au matériel de secours, en passant par les vêtements et les matériaux pour engins incendiaires. Cherchez des « sites de fabrication » sûrs où vous pouvez fabriquer les engins incendiaires sans laisser ni recueillir de traces. S'il n'y en a pas, achetez des tentes bon marché et installez-les là où vous vous sentez en sécurité. Ensuite, jetez la tente ou brûlez-la. Réfléchissez à toutes les étapes avant, pendant et après l'action, encore et encore, et demandez-vous si vous risquez de laisser des traces quelque part ou d'être inquiété après coup.

Dans une affaire contre plusieurs camarades, l'enquête montre que les flics ont utilisé un dispositif de localisation GPS dans l'un de leurs vélos. Plusieurs opérations de surveillance contre le camarade et son environnement immédiat sont suggérées, sans qu'on sache si ces opérations ont eu lieu via une caméra installée à son domicile, par une équipe de surveillance ou autre. La police de sécurité du pays étant chargée de mener l'enquête, de nombreuses informations manquent de détails.

Attardons-nous sur le vélo. Cette forme de surveillance, qui consiste à placer et installer secrètement un dispositif de localisation GPS dans les cavités du vélo, s'effectue dans un contexte où ça fait déjà partie des procédures de sécurité de fouiller les vélos privés afin d'éviter ce scénario particulier, notamment pour ne pas attirer les flics dans les réunions ou les séances de repérages. À moins que le camarade n'ait été négligent, utilisant son

propre vélo sans le fouiller—nous ne pouvons pas le savoir pour l'instant, le camarade étant toujours prisonnier de la cage en béton de l'ennemi—il se peut que les flics dissimulent mal leurs appareils. Mais le plus probable est que le camarade n'a pas volé ou emprunté un vélo et qu'il n'a pas détaché le guidon et la selle pour fouiller les cavités avec une lampe, ses doigts et d'autres outils appropriés. La leçon ? Ne jamais utiliser son propre vélo dans une attaque ou tout ce qui a trait à une attaque contre l'ennemi. Fouillez le vélo à intervalles réguliers, mais surtout avant une action, pour voir si des mesures de sécurité supplémentaires sont nécessaires.

Les auteur·e·s de ce texte font partie de celleux qui souhaitent la mort d'Internet, ainsi que de la civilisation et de toutes les infrastructures qui permettent sa survie et son expansion. En même temps, nous l'utilisons sans cesse. Parfois, nous faisons des erreurs, mais il y a une chose sur laquelle nous ne faisons jamais d'erreur : nous ne communiquons jamais par voie numérique sur quelque chose que nous ne pourrions pas dire directement à un flic ou à un procureur. Peu importe que ce soit chiffré ; avec PGP, par Signal, Telegram ou OTR, ou même dans des brouillons d'adresses email secrètes. Nous n'utilisons pas de smartphones, ni en privé, ni lors des actions. Il est possible d'utiliser Signal sur un ordinateur, par exemple, mais si nous le faisons, c'est pour cacher nos liens sociaux, pas pour conspirer.

Selon nous, la base pour vous épargner beaucoup d'ennuis à vous et à vos camarades, dans la vie de tous les jours comme lors d'une perquisition, est d'organiser votre vie numérique de la manière suivante (ou similaire) :

- Un ordinateur pour les affaires privées : navigation sur le web, envoi d'emails, visionnage de films, etc. De préférence sur un système Linux chiffré.
- Un ordinateur avec des systèmes Tails persistants pour contacter des camarades, pour des projets, pour une éventuelle collecte d'informations et l'édition ou la rédaction de textes, d'images, etc.
- Si des revendications d'action doivent être écrites : avoir un ordinateur supplémentaire sans interface réseau, et l'utiliser avec Tails pour écrire. Ne publiez jamais à partir d'un ordinateur ou d'un réseau qui peut être relié à vous.

- Si vous avez des disques durs externes : chiffrez-les avec Veracrypt ou avec les options de chiffrement de Linux.
- Si l'État parvient à s'introduire dans votre système, avec des logiciels malveillants, etc., le chiffrement et les autres mesures de sécurité ne seront d'aucune utilité, car à ce stade-là, vous avez probablement déjà un enregistreur de frappe (keylogger) d'installé. Pour réduire ce risque : utilisez Linux, n'ouvrez jamais d'emails inconnus et faites attention à ce que vous téléchargez sur votre ordinateur.
- Pendant une perquisition, débranchez/éteignez tous les appareils électroniques dotés d'un disque dur, d'une carte mémoire ou d'une carte réseau.

Il existe une multitude de textes approfondis sur le sujet, il ne s'agit donc que d'un petit post-it.

Enfin, nous voulons juste souligner que notre objectif n'est pas de rendre aussi difficile, complexe, ennuyeux ou exigeant que possible d'agir, d'attaquer physiquement le monde qui nous prive de notre liberté. Chaque situation requiert sa propre analyse, ses propres méthodes et expériences, et nos propositions peuvent être complètement hors de propos. En même temps, nous avons appris de générations de lutte ce que l'ennemi a dans son arsenal et nous avons essayé de voir au-delà. Nous essayons d'apprendre de nos erreurs et de celles des autres camarades, mais également de nos succès et de ceux des autres camarades.

D'une part : qu'est-ce qui est possible malgré la surveillance intensive et les capacités de la police scientifique ? D'autre part, quelles sont les brèches où ils n'ont pas encore réussi à développer ou à tester leurs méthodes répressives ? Nous nous battons par désir et par envie, nous devons vouloir défier leur répression et nous défier nous-même, sinon cela ne sert à rien de se battre. L'ennemi ne peut pas être partout et tout le temps. Les ombres nous appartiennent.

Il existe de nombreux guides qui décrivent toutes sortes de choses, depuis les meilleurs moyens de fabriquer des engins incendiaires à retardement à la gestion des traces ADN, en passant par les techniques pour contrer la police scientifique et les manières de protéger des données numériques face aux perquisitions, aux saisies ou à la surveillance gouvernementale. Certains d'entre eux ont plus de quarante ans, d'autres sont plus récents, certains sont encore valables, d'autres doivent être mis à jour. Nous avons pensé que ça ne ferait pas de mal de rassembler quelques suggestions, un article pas trop long avec des « trucs à prendre en considération », qui soit raisonnablement en phase avec les méthodes de l'ennemi.

No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

Selon votre contexte, la possession de certains documents peut être criminalisée ou attirer une attention indésirable—faites attention aux brochures que vous imprimez et à l'endroit où vous les conservez.