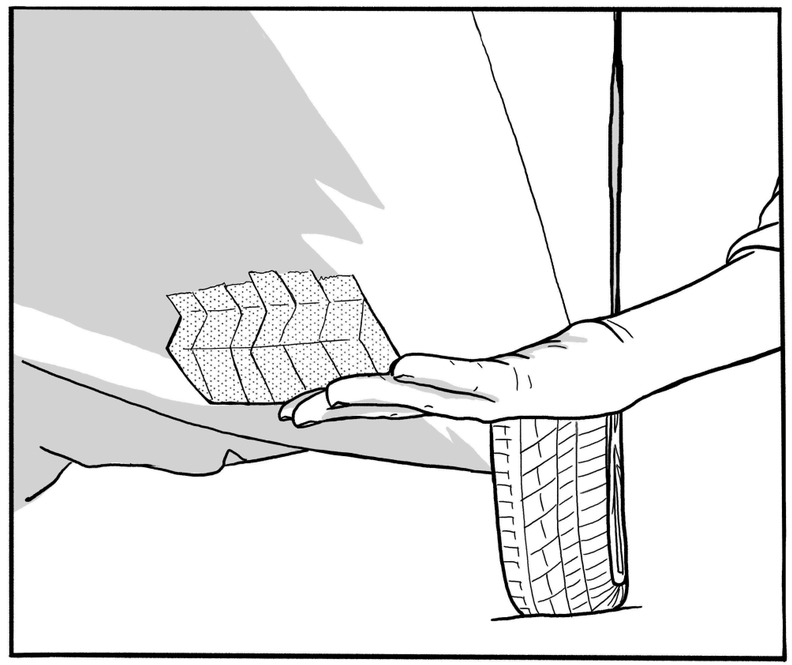
Bibliothèque de menaces

Partie 1/2

Tutoriel, Tactiques

Techniques



La Bibliothèque de menaces est une base de connaissances de techniques répressives utilisées par les ennemis des anarchistes et autres rebelles et d'opérations répressives où elles ont été utilisées—une analyse et classification des actions qui peuvent être utilisées contre nous. Son but est de t'aider à réfléchir aux mesures d'atténuation à mettre en place pour un projet donné et à parcourir des ressources qui abordent ces sujets plus en profondeur. Autrement dit, elle t'aide à aboutir à une sécurité opérationnelle adaptée à ton modèle de menace.

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.

Bibliothèque de menaces
Partie 1/2 : Tutoriel, Tactiques, Techniques
Partie 2/2 : Mesures d'atténuation, Opérations répressives, Pays

Publication originale du No Trace Project

notrace.how/threat-library/fr

Cette brochure est divisée en plusieurs parties. Les chapitres dans la partie actuelle sont référencés par leurs numéros de page. Les chapitres dans d'autres parties sont référencés par le symbole # suivi du numéro de la partie.

11 juillet 2024

Un résumé des mises à jour depuis cette date est disponible sur :
notrace.how/threat-library/fr/changelog.html

Une visite discrète de domicile est une visite secrète d'une résidence effectuée par un adversaire lorsque les occupant·e·s ne sont pas présents.

Un adversaire peut faire une visite discrète de domicile pour :

- Rassembler des informations.
- Cacher des **dispositifs de surveillance (p. 21)** dans le domicile.
- Installer des **malware (p. 46)** sur des appareils numériques.

Généralement, quand un adversaire fait une visite discrète de domicile, il ne veut pas que les occupant·e·s sachent que l'opération a eu lieu. Ainsi, en général :

- Si le domicile a des portes verrouillées, l'adversaire doit passer les portes sans les abîmer de manière visible. Il peut faire ça en crochetant la serrure ou en demandant les clés au propriétaire du bâtiment.
- L'adversaire s'abstient de saisir des objets ou de bouger des choses.

En plus de visiter le domicile, l'adversaire peut saisir discrètement les poubelles à l'extérieur du domicile dans l'espoir d'y trouver des informations intéressantes (par exemple des notes écrites ou des preuves forensiques comme des traces ADN).

Mesures d'atténuation

Cachette ou planque (#2) : Tu peux garder du matériel d'action qui n'a pas de fonction « légitime » dans une cachette ou une planque, ou, au pire, le laisser transiter chez toi seulement pendant très peu de temps.

Clandestinité (#2) : SI tu entres en clandestinité, un adversaire ne peut pas savoir où tu vis, et ne peut donc pas faire une visite discrète de ton domicile.

Détection d'intrusion physique (#2) : Tu peux prendre des mesures de détection d'intrusion physique pour détecter une visite discrète de domicile.

Se préparer aux perquisitions (#2) : Tu peux te préparer pour une visite discrète de domicile en minimisant la présence d'objets qui pourraient être problématiques en cas de visite.

Opérations répressives

Opération contre Peppy et Krystal (#2) : Les enquêteurs ont secrètement fouillé la poubelle devant le domicile de Peppy et Krystal, où ils ont trouvé des documents suspects[19].

tralisé des vigiles en les désarmant[114], en les ligotant[115] ou en leur tirant dessus[116].

Reconnaissance (#2) : Avant une action, tu peux déterminer si des vigiles sont présents sur le lieu de l'action.

4.25. Violence physique

Utilisée par les tactiques : **Dissuasion (p. 15)**, **Incrimination (p. 15)**

La violence physique est l'utilisation de la force physique par un adversaire pour intimider une cible ou son réseau, empêcher une cible de poursuivre ses activités, ou contraindre une cible à révéler des informations.

Dans certains contextes, la violence physique peut inclure de la torture. Par exemple, en Russie et Biélorussie, plusieurs anarchistes ont été torturés ces dernières années après avoir été arrêtés par l'État. Les actes de tortures constatés dans ces pays incluent :[117].

Dans certains contextes, la violence physique peut inclure des assassinats.

Mesures d'atténuation

Se préparer à la répression (#2) : Si toi, ou des membres de ton réseau, risquez d'être torturés si vous êtes arrêtés, vous pouvez vous préparer à ce risque. Par exemple :

- Vous pouvez vous préparer psychologiquement.
- Vous pouvez mettre en place à l'avance des protocoles qui permettent au réseau de remarquer la disparition d'une personne pour pouvoir y réagir rapidement. Par exemple, des membres d'un groupe peuvent se connecter chaque jour à une application de messagerie chiffrée pour s'envoyer un message les un·e·s aux autres : si un·e membre n'envoie pas son message quotidien, cela peut signifier qu'iel a été arrêté·e. La torture se produit souvent immédiatement après l'arrestation, quand personne ne sait où est la personne et qu'il n'y a pas d'avocat, donc réagir rapidement après l'arrestation peut être crucial.
- En fonction du contexte, impliquer un avocat ou rendre publics les actes de torture peut aider à faire pression sur les autorités pour qu'elles arrêtent la torture.

Opérations répressives

Network (#2) : La plupart des accusé·e·s ont été torturé·e·s par le Service fédéral de sécurité de la fédération de Russie (FSB) au début de leurs détentions pour obtenir des déclarations (souvent falsifiées) qui pourraient ensuite être utilisées pour les incriminer et les condamner[118]. La plupart des accusé·e·s qui ont été torturé·e·s ont plus tard renié leurs déclarations et dénoncé publiquement la torture qui leur a été infligée.

Renata (#2) : Pendant une perquisition, une des personnes arrêté·e·s a été forcée de se mettre à genoux par un policier qui a pointé un pistolet contre sa tempe[48].

Partisans anarchistes biélorusses (#2) : Les personnes ont été torturées dans les premiers jours de leur détention[119].

Les trois de Varsovie (#2) : Les personnes ont été torturées pendant leur arrestation et les premières heures de leur détention[113].

Répression du soulèvement de 2019 au Chili (#2) : Dans les rues et en garde-à-vue, les policiers et soldats ont blessé, agressé sexuellement, violé, torturé et tué de nombreuses manifestant·e·s, vraisemblablement dans une volonté stratégique de dissuader les manifestant·e·s de participer au soulèvement[103].

4.26. Visite discrète de domicile

Utilisée par les tactiques : **Incrimination (p. 15)**

[114] https://actforfree.noblogs.org/post/2022/08/04/chile-a-fiery-july-in-the-mapuche-territories

[115] https://actforfree.noblogs.org/post/2022/02/28/chile-the-mapuche-struggle-continues-under-a-state-of-emergency

[116] https://actforfree.noblogs.org/post/2021/07/21/chile-mapuche-zone-ignites-after-the-murder-of-pablo-marchant-update

[117]

des tabassages, la suffocation avec un sac en plastique ou un oreiller, de l'eau versée dans le nez et la bouche, la suspension par les jambes ou par les mains, des décharges électriques, la torture avec un tournevis, forcer des personnes à faire des squats jusqu'à ce qu'elles s'écroulent, des violences sexuelles, et la privation de sommeil, de nourriture et d'eau.

[118] https://web.archive.org/web/20210724133854/https://a2day.net/network-underground

[119] https://pramen.io/en/2021/12/blood-on-your-hands-regarding-information-about-torture-of-anarcho-partisans

Sommaire

Affaire du 8 décembre (#2) : En interrogeant les inculpé·e·s en garde-à-vue, les enquêteurs ont[37] :

- Prétendu que les inculpé·e·s ne seraient pas poursuivis s'ils dénonçaient les autres inculpé·e·s, ce qui était un mensonge.
- Menacé un·e des inculpé·e·s d'agression sexuelle.

4.23. Vérifications d'identité

Utilisée par les tactiques : **Arrestation (p. 15)**, **Incrimination (p. 15)**

Une vérification d'identité est le processus par lequel l'État vérifie l'identité d'une personne en lui demandant ses informations personnelles, en lui demandant de présenter un document d'identité officiel, ou en collectant ses informations biométriques (photo du visage, empreintes digitales, ADN) et en les comparant avec une base de données. Une vérification d'identité peut être un prétexte pour un interrogatoire et des pressions, et peut être suivi d'une fouille des affaires de la personne.

Se soumettre à un contrôle d'identité donne à l'État des informations à ton propos, ce qui peut l'aider à **cartographier ton réseau (p. 16)**, et peut mener à ton arrestation si il te recherche. Les conséquences d'un refus ou d'une incapacité à se soumettre à un contrôle d'identité dépendent fortement du contexte, mais peuvent inclure avoir tes informations biométriques collectées de force ou à ton insu, être détenu, et être expulsé hors du pays.

La probabilité d'être ciblé par un contrôle d'identité dépend de la situation et de comment tu es perçu·e par l'État. Il est moins probable que tu sois ciblé·e si tu ne fais rien de remarquable et que tu es habillé·e comme un·e bourgeois·e. Il est plus probable que tu sois ciblé·e si tu es perçu·e comme un·e potentiel·le criminel·le ou migrant·e illégal·le, ou si tu es en train de rejoindre ou de quitter une émeute.

Mesures d'atténuation

Fausse identité (#2) : Pendant une vérification d'identité, si fournir ton identité réelle pourrait mener à ton arrestation ou d'autres conséquences négatives, tu peux présenter une fausse identité (tant que la fausse identité n'est pas reconnue comme telle par l'État).

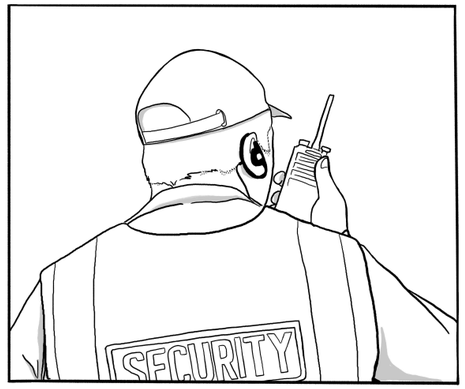
Éviter l'auto-incrimination (#2) : Si possible, tu peux éviter de répondre à des questions ou de fournir tes informations biométriques (photo du visage, empreintes digitales, ADN) pendant une vérification d'identité.

Opérations répressives

Opération contre Boris (#2) : Les enquêteurs ont obtenu et analysé l'historique des contrôles d'identité faits par la police peu de temps avant et après les sabotages, dans différents périmètres autour de là où les sabotages ont eu lieu, en espérant vraisemblablement trouver les noms des saboteurs dans cet historique[22].

4.24. Vigiles

Utilisée par les tactiques : **Arrestation (p. 15)**



Les vigiles (aussi connus sous le nom d'*agents de sécurité*) sont des personnes employées par un adversaire pour protéger des bâtiments ou autres infrastructures physiques.

Si des vigiles détectent une présence non autorisée dans la zone qu'ils surveillent, ils peuvent décider d'intervenir eux-mêmes ou d'appeler à l'aide. En fonction du contexte, ils peuvent être équipés d'armes léthales ou non-léthales.

Mesures d'atténuation

Attaque (#2) : Avant ou pendant une action, tu peux immobiliser des vigiles pour les empêcher t'interférer avec l'action. Par exemple, dans leurs actions contre les machines d'entreprises d'exploitation forestière sur le territoire contrôlé par l'État chilien, des Mapuches ont neu-

teurs peuvent être des détecteurs de mouvement à infrarouge, des capteurs qui détectent l'ouverture des portes, et de nombreux autres types de capteurs[109]. Le signal d'alerte peut être transmis par une connexion filiaire ou sans fil—les systèmes modernes bon marché envoient souvent le signal sur le réseau téléphonique.

Dans le cas des infrastructures numériques, les systèmes de détection d'intrusion[110] tentent de détecter toute activité qui puisse indiquer qu'un piratage est en cours. Si un accès non autorisé est détecté, une équipe d'intervention dédiée peut être alertée dans le but de contenir et de remédier à tout compromis.

Mesures d'atténuation

Attaque (#2) : Tu peux attaquer des systèmes d'alarme ou les lignes de communication qu'ils utilisent pour envoyer des signaux d'alerte. Par exemple, tu peux détruire des systèmes d'alarme ou brouiller les signaux d'alerte avec un dispositif de brouillage.

Certains systèmes d'alarme fonctionnent en envoyant des signaux périodiquement ou en continu, même si rien d'anormal n'est détecté. Dans de tels cas, si tu attaques un système d'alarme de telle manière que ses signaux sont interrompus, cela pourrait être interprété comme une alerte et déclencher une intervention.

Bonnes pratiques numériques (#2) : Quand tu effectues une cyber-action, tu peux utiliser des techniques d'évasion numérique[111] pour empêcher les systèmes de détection d'intrusion de détecter l'action.

Reconnaissance (#2) : Avant une action, tu peux inspecter le bâtiment ou l'infrastructure ciblé pour évaluer la présence ou l'absence de systèmes d'alarme, et le type et l'emplacement des capteurs et autres dispositifs d'alarme.

4.22. Techniques d'interrogatoire

Utilisée par les tactiques : **Incrimination (p. 15)**

Les techniques d'interrogatoire sont les méthodes utilisées par un adversaire pour obtenir des informations en interrogeant des gens.

Les techniques d'interrogatoire peuvent inclure le mensonge, les menaces, inspirer de la culpabilité, de la honte ou de la fierté, essayer d'apparaître amical et aimable ou, au contraire, menaçant et violent, etc. Dans certains cas, elles peuvent inclure de la **violence physique (p. 53)**.

Voir Comment la police interroge et comment s'en défendre[112] pour une vue d'ensemble complète des techniques d'interrogatoire de la police.

Mesures d'atténuation

Éviter l'auto-incrimination (#2) : Tu ne devrais en aucun cas parler à un adversaire : c'est le meilleur moyen de résister à ses techniques d'interrogatoire.

Opérations répressives

Opération contre Boris (#2) : En interrogeant des personnes proches de Boris, les enquêteurs ont utilisé des mensonges élaborés pour essayer de les faire parler[22]. Par exemple, les enquêteurs suspectaient vaguement que les personnes interrogées avaient hébergé Boris en avril 2020 et voulaient confirmer leurs suspicions, et ont donc demandé, « Il ressort de nos investigations que vous avez hébergé [Boris] en avril 2020. Combien de temps l'avez vous hébergé ? »

Les trois de Varsovie (#2) : Quelques semaines après le début de sa détention, une personne a donné un témoignage « conséquent » à la police. Il a affirmé que c'était en partie à cause de deux techniques utilisées par l'un·e de ses avocats pour le pousser à donner ce témoignage[113]:

- L'avocat lui a montré une publication sur un réseau social rédigée par une personne de son milieu politique peu après son arrestation. La publication critiquait l'action pour laquelle il a été arrêté et n'incluait pas de déclaration de solidarité. Comme cette publication était la seule réaction en provenance de son milieu politique dont la personne a eu connaissance, il s'est senti isolé.
- L'avocat lui a dit que deux autres personnes avaient déjà donné des témoignages conséquents à la police, ce qui était un mensonge.

[109] https://en.wikipedia.org/wiki/Security_alarm#Sensor_types

[110] https://en.wikipedia.org/wiki/Intrusion_detection_system

[111] https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques

[112] https://notrace.how/resources/fr/#police-interroge

[113] https://wawa3.noblogs.org/post/2017/05/24/olsen-gang-replies-statements-of-warsaw-three-en

1. À propos de la Bibliothèque de menaces

> Quoi qu'il arrive, nous faisons et continuerons de faire des erreurs dans la lutte contre des mécanismes d'oppression aussi puissants. Des erreurs qui « coûteront » toujours plus cher par rapport aux erreurs des flics qui sont « absorbées ». Nous devons évaluer à nouveau les situations et veiller à ce que les erreurs commises une fois ne se reproduisent plus. Nous devons étudier et apprécier l'expérience accumulée depuis tant d'années et, en tenant compte de la tendance à se préparer pour les batailles qui ont déjà eu lieu et non pour celles qui viendront, soyons prêt·e·s et que la chance soit avec nous…
>
> — *camarades anarchistes de Grèce, dans un texte[1] détaillant la surveillance qui a conduit à leur arrestation, 2013*

1.1. Modélisation de menaces

La modélisation de menaces est un processus par lequel tu identifies de potentielles *menaces* en provenance de tes *adversaires* pour pouvoir ensuite identifier et prioriser les mesures d'atténuation que tu peux prendre face à ces menaces. La liste des menaces et leurs risques respectifs sont appelés *modèle de menace*.

Si tu fais des actions ou projets subversifs, tu as probablement déjà l'habitude de réfléchir à comment minimiser les risques posés par diverses menaces. La modélisation de menaces formalise ces réflexions pour les rendre plus organisées et systématiques.

1.2. La Bibliothèque de menaces

La Bibliothèque de menaces est un outil développé par le No Trace Project pour aider les anarchistes et autres rebelles à utiliser la modélisation de menaces dans leurs actions et projets. La Bibliothèque de menaces utilise quelques termes techniques avec lesquels tu voudras te familiariser :

- Un **adversaire** est une entité qui veut t'empêcher d'atteindre tes objectifs, de mener à bien tes actions et projets. Typiquement ton adversaire c'est l'État, mais selon ton contexte tu peux avoir d'autres adversaires (par exemples des groupes fascistes).
- Une **technique** (ou *menace*) est quelque chose qu'un adversaire fait pour t'empêcher d'atteindre tes objectifs.
- Une **mesure d'atténuation** est quelque chose que tu fais pour réduire le risque qu'une technique réussisse.
- Une **tactique** est l'objectif d'un adversaire lorsqu'il utilise une technique. Dans la Bibliothèque de menaces, les techniques sont organisées en trois tactiques : dissuasion, incrimination et arrestation.
- Une **opération répressive** est un cas réel de répression d'un adversaire contre des anarchistes ou autres rebelles.
- Une **action ou projet** est ce que tu veux accomplir : participer à une émeute, publier des écrits subversifs, casser un truc, brûler un truc…

La Bibliothèque de menaces contient de nombreuses informations sur les techniques répressives d'État. Cela peut avoir un effet paralysant, en faisant paraître l'État comme tout-puissant. L'État n'est pas tout-puissant[2]. L'intention de la Bibliothèque de menaces n'est ni de minimiser ni d'exagérer les capacités de l'État, mais plutôt de comprendre les options à sa disposition et comment ces options sont utilisées dans différents contextes.

1.3. Explorer la Bibliothèque de menaces

Il y a de nombreuses manières d'explorer la Bibliothèque de menaces :

- La page d'accueil[5] présente une vue d'ensemble de toutes les tactiques et techniques.

[1] https://notrace.how/resources/fr/#nea-filadelphia

[2] En réalité, la grande majorité des actions directes anarchistes ne sont pas poursuivies en justice. Des enquêteurs frustrés de Bremen, en Allemagne[3] et de Grenoble, en France[4] ont lamenté dans les médias leur incapacité à réprimer un seul des incendies volontaires qui ont eu lieu dans les deux villes au fil des années, phénomène qu'ils attribuent aux mesures d'atténuation prises par les incendiaires.

[3] https://notrace.how/resources/fr/#pas-stupides

[4] https://sansnom.noblogs.org/archives/11527

- Les **techniques (p. 16)**, **mesures d'atténuation (#2)**, et **opérations répressives (#2)** sont listées sur leurs pages respectives.
- Le **tutoriel de la Bibliothèque de menaces (p. 6)** est conçu pour t'aider à utiliser la Bibliothèque de menaces dans le contexte d'une action ou projet particulier.

1.4. Limites

La Bibliothèque de menaces a délibérement une approche très technique de l'anti-répression. La modélisation de menaces se fait au niveau des actions, et ne tente donc pas de contribuer à la question sociale, comment échapper à l'enfermement voulu par la répression, comment intervenir dans les tensions sociales, et ainsi de suite. Les luttes pour la liberté ne sont pas en premier lieu une affaire technique, mais une affaire sociale, et peuvent avoir des effets psychologiques et émotionnels. Autant que possible, nous t'encourageons à prendre du temps avant, pendant et après une action pour discuter avec toutes les personnes impliquées et t'assurer que les besoins émotionnels de chacun·e sont pris en compte.

La Bibliothèque de menaces cherche à répertorier d'une manière aussi complète que possible les menaces auxquelles les anarchistes et autres rebelles peuvent faire face, mais elle est pensée pour évoluer avec le temps et ne sera jamais exhaustive. Ceci est particulièrement vrai du fait que les adversaires peuvent développer des techniques nouvelles et inattendues. Pour éviter d'avoir un faux sentiment de sécurité en lisant la Bibliothèque de menaces, nous t'encourageons à utiliser d'autres sources d'information, à rester critique, et à toujours prendre en compte ton contexte personnel lorsque tu prends des décisions importantes.

[5] https://notrace.how/threat-library/fr

sortis de leur voiture pour continuer à pied, et l'équipe de surveillance les a perdus de vue. Ils sont revenus en courant vers leur voiture 10 minutes plus tard, et l'équipe de surveillance s'est remise à les observer. Ils ont quitté en voiture le lieu de l'incendie. Plus d'une heure plus tard, l'équipe de surveillance—qui suivait toujours les incendiaires—a entendu parler, sur le système de communication radio de la police, d'un feu sur le lieu de l'incendie et a demandé à des policiers locaux d'arrêter la voiture des incendiaires pour un contrôle routier, suspectant qu'ils avaient quelque chose à voir avec le feu. Une demi-heure plus tard, quand les experts incendie sur le lieu de l'incendie ont indiqué qu'ils pensaient que le feu était d'origine volontaire, les incendiaires ont été arrêtés.

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs[13] :

- Ont suivi l'une des personnes arrêtées pendant quelques heures une fois, et pendant quelques minutes une autre fois, pour découvrir où elle habitait.
- Ont passé plusieurs jours à faire une surveillance statique d'un lieu associé à la lutte contre Cigéo appelé l'« ancienne gare de Luméville », quelques bâtiments isolés entourés par des champs. Pendant jusqu'à 16 heures par jour ils ont noté et photographié les personnes et véhicules rejoignant et quittant le lieu.

Les trois du banc public (#2) : Au cours de la soirée précédant l'arrestation, deux des personnes ont roulé en vélo à travers la ville et ont été suivies par des policiers en vélo (et probablement aussi des policiers en voiture) jusqu'à leur arrestation dans le parc[78]. Les policiers ont décidé de suivre les personnes ce soir là en particulier car cela faisait exactement deux ans depuis le sommet du G20 à Hambourg et qu'elles étaient suspectées de prévoir une action pour l'anniversaire du sommet.

Opération à Nea Filadelphia (#2) : Le jour des arrestations, quand une personne a visité un cybercafé qui était probablement sous surveillance policière, des policiers l'ont reconnue et se sont mis à la suivre[107]. Elle s'est ensuite déplacée à travers les rues d'Athènes pendant quelques heures, rejoignant petit à petit les autres personnes—dont certaines étaient recherchées par la police[108]—et tout le monde a été arrêté.

4.20.3. Visible

La surveillance physique visible est l'observation directe de personnes ou d'activités quand les opérateurs de surveillance ont l'intention d'être détectés par leurs cibles, ou que ça ne les dérange pas d'être détectés par leurs cibles. Il s'agit d'une pratique courante lors de manifestations et rassemblements pour identifier les participants, que ce soit pour faire de la **cartographie de réseau (p. 16)** ou pour incriminer des personnes pour des actions réalisées pendant la manifestation.

La surveillance physique visible de seulement quelques individus est rare, et a plus souvent pour objectif de créer de la paranoïa pour dissuader que d'incriminer.

Mesures d'atténuation

Tenue anonyme (#2) : Tu peux porter une tenue anonyme dans une manifestation ou autre évènement pour que ce soit plus difficile pour une opération de surveillance visible de t'identifier.

Opérations répressives

Mauvaises intentions (#2) : Pendant une manifestation, les enquêteurs ont pris 180 photos, à partir desquelles ils ont obtenu 200 portaits des manifestant·e·s, dont dix personnes qu'ils ont pu identifier[11].

4.21. Systèmes d'alarme

Utilisée par les tactiques : **Arrestation (p. 15)**

Les systèmes d'alarme sont des mécanismes qui protègent les infrastructures physiques ou numériques en envoyant un signal d'alerte quand un accès non autorisé à l'infrastructure est détecté. Le signal d'alerte peut mener à l'intervention rapide d'agents de sécurité ou de la police pour investiguer la situation.

Dans le cas des infrastructures physiques, les systèmes d'alarme modernes comportent typiquement des capteurs qui détectent l'accès non autorisé à une zone en dehors des horaires de fonctionnement habituels. Ces cap-

[107] https://web.archive.org/web/20201027031238/http://actforfree.nostate.net/?p=15472

[108] https://machorka.espivblogs.net/2013/11/06/letter-from-anarchists-argiris-dalios-and-fivos-harisis-from-koridallos-prisons-athens

- Faire tourner l'opérateur ou le véhicule de surveillance le plus proche de la cible pour limiter le risque que la cible remarque qu'elle est suivie.

La surveillance physique mobile peut être facilitée par :

- Un **dispositif de surveillance par localisation (p. 23)** installé sur le véhicule ou le vélo de la cible.
- Une **surveillance aérienne (p. 47)**, par exemple un drone qui suit la cible de loin.

Statique

La surveillance physique statique est l'observation d'une cible quand la cible ne peut pas bouger, ou que les opérateurs de surveillance n'ont pas l'intention de la suivre si elle bouge. Une opération de surveillance physique statique est typiquement menée par une équipe de surveillance utilisant un ou plusieurs véhicules.

Un exemple d'une opération de surveillance physique statique est de garer un véhicule de surveillance devant le domicile d'une cible, avec des opérateurs de surveillance à l'intérieur du véhicule observant l'entrée du domicile.

Arrestation

Généralement, une équipe de surveillance ne va pas tenter d'arrêter sa cible au cours d'une opération de surveillance physique cachée. Dans de rares cas, cependant, cela peut se produire si l'équipe de surveillance a obtenu suffisamment d'informations sur les activités de la cible pour l'incriminer et juge nécessaire d'arrêter la cible immédiatement (par exemple pour l'empêcher de commettre un crime).

Voir aussi

- Surveillance Countermeasures[104] (*Mesures contre la surveillance*) à propos des principes et techniques de la surveillance physique cachée.
- Maßnahmen gegen Observation[105] (*Mesures contre la surveillance*) pour un aperçu de comment les agences de police et de renseignement pratiquent la surveillance physique cachée.
- Le sujet « Surveillance physique »[106].

[104]https://notrace.how/resources/fr/#surveillance-countermeasures

[105]https://notrace.how/resources/fr/#gegen-observation

Mesures d'atténuation

Anti-surveillance (#2) : Tu peux faire de l'anti-surveillance pour échapper à une opération de surveillance physique cachée.

Déplacement en vélo (#2) : Tu peux utiliser un vélo plutôt qu'un autre type de véhicule : comparé aux autres véhicules ou à des personnes à pied, un vélo est plus difficile à suivre par une opération de surveillance physique cachée, surtout sans que l'opération soit détectée.

Détection de surveillance (#2) : Tu peux faire de la détection de surveillance pour détecter une opération de surveillance physique cachée.

Opérations répressives

Opération contre Boris (#2) : Pendant plusieurs semaines, les enquêteurs ont régulièrement surveillé le domicile de Boris et l'ont suivi lorsqu'il se déplaçait à pied, à vélo, et dans des véhicules[22].

Opération contre Peppy et Krystal (#2) : Une semaine avant la manifestation, les enquêteurs ont mis en place une surveillance physique discrète d'une bibliothèque locale où ils savaient que des personnes qui planifiaient la manifestation s'organisaient[19]. Ils ont observé Peppy entrer dans la bibliothèque et en partir une heure et demie plus tard.

Quelques jours après la manifestation, les enquêteurs ont mis en place une surveillance physique discrète du domicile de Peppy et Krystal. Ils ont observé Peppy et Krystal conduire la même moto qu'iels avaient utilisée pour arriver au lieu de la manifestation et en partir.

Répression du premier incendie de Jane's Revenge (#2) : En mars 2020, des policiers ont observé secrètement la personne à une distance d'environ 30 mètres[58]. Les policiers ont regardé la personne jeter un sac, l'ont récupéré, et ont prélevé des preuves ADN reliant la personne au lieu de l'action.

Opération contre Jeff Luers (#2) : La nuit de l'incendie de juin, les incendiaires étaient suivis par une équipe de surveillance—des policiers dans une ou plusieurs voitures en civil—alors qu'ils conduisaient vers le lieu de l'incendie[51]. Ils ont garé leur voiture proche du lieu de l'incendie, sous l'oeil de l'équipe de surveillance. Ils sont

[106]https://notrace.how/resources/fr/#topic=physical-surveillance

2. Tutoriel : utilisation de la Bibliothèque de menaces avec des arbres d'attaque

La Bibliothèque de menaces contient beaucoup d'informations. Ça peut être un peu écrasant. Comment est-ce que tu peux utiliser la Bibliothèque de menaces dans ta vie, dans un projet particulier, ou quand tu fais des actions ? Ce tutoriel est conçu pour t'aider à utiliser la Bibliothèque de menaces avec des *arbres d'attaque*[6].

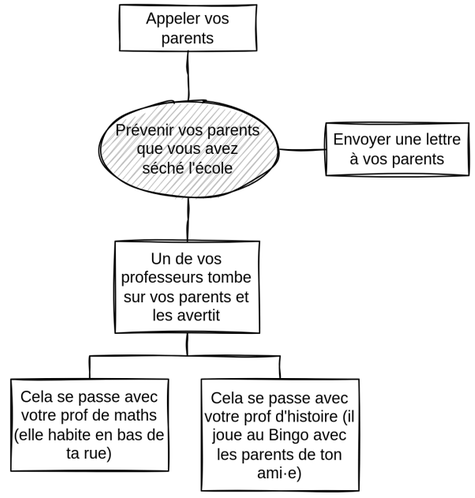
Les arbres d'attaque sont un outil pour t'aider à réfléchir aux différentes manières dont un adversaire pourrait t'attaquer avec succès dans un contexte donné, en représentant les attaques—les menaces—sous la forme d'un arbre. Ils aident à comprendre comment un plan ou projet est vulnérable à la répression en modélisant les options à la disposition d'un adversaire.

Tu peux faire cet exercice de *modélisation de menaces* seul·e mais, si tu prévois de faire une action avec d'autres personnes, nous te conseillons de le faire avec elles. Cet exercice devrait être bénéfique peu importe l'expérience du groupe. Même si tout le monde a déjà de bonnes pratiques de sécurité, il propose une approche structurée qui permet de s'assurer qu'aucune menace n'est négligée et que tout le monde est sur la même longueur d'ondes en terme d'attentes relatives à la sécurité.

2.1. Un exemple simple : sécher un jour d'école

Commençons avec un exemple simple avant de réfléchir à un vrai exemple. Tu es un·e gosse à l'école, et toi et ton ami·e voulez sécher un jour d'école, mais vous ne voulez pas que vos parents soient au courant. L'adversaire est le système scolaire.

Tu commences par dessiner le nœud racine : il représente l'objectif de l'adversaire. Dans cet exemple, l'objectif est de prévenir vos parents que vous avez séché l'école. L'école pourrait appeler vos parents ou leur envoyer une lettre. Ou un de vos profs pourrait tomber sur vos parents respectifs et les prévenir—ça pourrait se passer avec ta prof de maths qui vit en bas de ta rue, ou avec ton prof d'histoire qui joue au bingo avec les parents de ton ami·e tous les week-ends. Tu dessines tous ces nœuds (1).



(1) Arbre d'attaque « Sécher l'école ».

Pour qu'un nœud soit vrai, l'un de ses successeurs doit être vrai. Par exemple, pour que « Prévenir vos parents que vous avez séché l'école » soit vrai, l'un des trois nœuds autour de lui doit être vrai. Pour que « Un de vos professeurs tombe sur vos parents et les avertit » soit vrai, l'un des deux nœuds en-dessous de lui doit être vrai. Autrement dit, si tu peux tracer un chemin depuis un des nœuds les plus à l'extérieur jusqu'au nœud racine et que tous les nœuds du chemin sont vrais, alors le nœud racine est vrai, et l'attaque est réussie.

Donc toi et ton ami·e décidez de sécher un jour où vous n'avez ni maths ni histoire. La nuit avant de sécher, vous coupez les lignes téléphoniques de vos parents (vous accuserez les souris) et interceptez leur courrier les jours suivants. Vous êtes ravis d'avoir imaginé un super plan.

[6]Pour une autre approche de la modélisation de menaces qui peut aussi service de tutoriel à la Bibliothèque de menaces, voir Threat Modeling Fundamentals[7] (*Les bases de la modélisation de menaces*).

[7]https://notrace.how/resources/fr/#threat-modeling

2.2. Un vrai exemple : une émeute dans une grande ville des États-Unis

Disons que toi et quelques camarades vous vous préparez pour une émeute dans une grande ville des États-Unis. Vous voulez faire des dégâts, mais vous ne voulez pas vous faire prendre… Tu te tournes vers la Bibliothèque de menaces. Tu imprimes cette brochure, tu prends du papier et un crayon, et tu retrouves tes camarades **en extérieur et sans appareils électroniques (#2)**.

L'objectif de la discussion : dessiner un arbre d'attaque, identifier les techniques et mesures d'atténuation qui s'appliquent à votre contexte, et décider comment implémenter ces mesures d'atténuation. Après l'émeute, ça peut être une bonne idée de faire un *débriefing de l'action*.

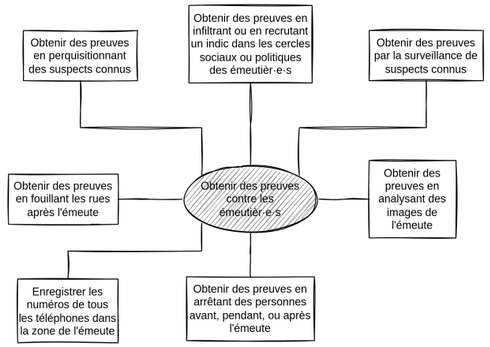
2.2.1. Dessiner l'arbre d'attaque

Dans cet exemple, l'adversaire est l'État et la police, et son but est d'obtenir suffisamment de preuves de votre participation à l'émeute pour convaincre un juge de vous condamner. Vous dessinez un arbre d'attaque pour représenter comment il pourrait atteindre cet objectif[8]. Vous commencez avec le nœud racine (2).

(2) Arbre d'attaque « Émeute » (nœud racine).

Vous ajoutez ensuite les nœuds les plus proches, à côté du nœud racine (3). À ce stade, vous devriez ajouter tout ce qui vous passe par la tête, même si vous n'êtes pas sûr·e·s que ça s'applique à votre contexte. Vous pouvez agrandir l'arbre dans toutes les directions, pour le rendre plus compact.

[8]Pour des actions complexes, on peut vouloir faire une distinction temporelle et dessiner un arbre d'attaque pour chaque étape de l'action (par exemple planification, préparation, exécution, dispersion).



(3) Arbre d'attaque « Émeute » (premiers nœuds).

Vous utilisez la Bibliothèque de menaces pour vous aider à agrandir l'arbre—vous renseigner sur les techniques vous aide à mieux comprendre les options à la disposition de votre adversaire. Créer des arbres d'attaque demande un certain état d'esprit et un peu d'expérience. L'arbre est complet quand il n'y a plus besoin de nœuds pour compléter une attaque, et que toutes les attaques auxquelles vous pensez sont représentées (4).

seconde, permettant de reconstruire au ralenti presque tout mouvement en extérieur[97], avec des images de haute qualité de nuit[98].

Voir le sujet « Surveillance aérienne »[99].

Mesures d'atténuation

Anti-surveillance (#2) : Tu peux inclure dans un itinéraire d'anti-surveillance des endroits qui empêcheraient une opération de surveillance aérienne de te suivre : un métro souterrain, un centre commercial avec beaucoup d'entrées, etc.

Attaque (#2) : Pendant une manifestation, tu peux abattre des drones avec des feux d'artifice, les pirater, ou les aveugler avec des lasers. Voir aussi Cinq manières à la portée de tous pour abattre un drone[100].

Détection de surveillance (#2) : Tu peux faire de la détection de surveillance pour détecter la plupart des hélicoptères et certains drones en tendant l'oreille à de potentiels hélicoptères et drones : tu devrais entendre la plupart d'entre eux, selon leur altitude et l'endroit où tu te trouves.

Tenue anonyme (#2) : Si tu es suivi·e par une opération de surveillance aérienne, tu peux te changer et mettre une tenue anonyme quand tu es dans un endroit qui n'est pas visible depuis le ciel pour que ce soit plus difficile pour l'opération de surveillance aérienne de te retrouver quand tu émergeras dans un endroit visible (ça ne fonctionnera pas si l'opération de surveillance t'observe également depuis le sol).

Opérations répressives

Conspiration sur un chemin de fer à Berlin en 2023 (#2) : Les personnes arrêtées ont été découvertes de nuit par un hélicoptère au cours d'un vol de surveillance de routine, vraisemblement muni d'équipement de vision nocture[101]. Un texte[102] relate qu'en 2022, lors d'un autre vol de surveillance de routine près de Berlin, ce même hélicoptère avait éteint ses feux de navigation et étouffé le son des pales de son rotor pour éviter d'être détecté : « Bien qu'on puisse toujours entendre l'hélicoptère, il faisait moins de bruit. Cela peut mener à sous-estimer la distance de l'hélicoptère, ou, si d'autres bruits sont présents comme une autoroute, à ne pas se rendre compte du problème en approche avant qu'il ne soit trop tard. »

Répression du soulèvement de 2019 au Chili (#2) : Des drones ont été utilisés pour suivre les émeutièr·e·s qui quittaient les émeutes pour pouvoir les arrêter[103].

[97]https://theintercept.com/2020/04/09/baltimore-police-aerial-surveillance

[98]https://theintercept.com/document/2021/08/31/motion-to-suppress-aerial-surveillance-evidence-in-u-s-vs-muhammed-momtaz-alazhari

[99]https://notrace.how/resources/fr/#topic=aerial-surveillance

[100]https://notrace.how/resources/fr/#cinq-manieres

[101]https://notrace.how/resources/fr/#on-conspire

[102]https://kontrapolis.info/9821

4.20.2. Cachée

La surveillance physique cachée est l'observation directe de personnes ou d'activités quand les opérateurs de surveillance ne veulent pas être détectés par leurs cibles.

Mobile

Une opération de surveillance physique mobile est typiquement menée par une équipe de surveillance de cinq à vingt opérateurs utilisant plusieurs véhicules, et commence typiquement par une phase statique : surveiller l'endroit où la cible est présumée se trouver, comme son domicile ou son lieu de travail. Quand la cible quitte la zone de surveillance statique, l'équipe de surveillance se met à la suivre et l'opération de surveillance transitionne vers une phase mobile. L'opération de surveillance alterne ensuite entre des phases statiques (quand la cible s'arrête) et des phases mobiles (quand la cible se remet en mouvement).

Voici des exemples de techniques de surveillance physique mobile :

- Utiliser un moyen de transport approprié en fonction du moyen de transport de la cible. Par exemple, si la cible est dans un véhicule, l'équipe de surveillance doit utiliser des véhicules, mais si la cible est à pied, l'équipe de surveillance peut préférer utiliser des opérateurs à pied.
- Se mettre à couvert et se dissimuler pour éviter d'être détecté par la cible. Par exemple, des véhicules de surveillance peuvent se cacher derrière d'autres véhicules, et des opérateurs de surveillance à pied peuvent se cacher parmi les autres piétons.

[103]https://es-contrainfo.espiv.net/2019/11/06/chile-una-mirada-anarquica-al-contexto-de-revuelta-y-represion

Parce que la plupart des sites web, fournisseurs d'email, et applications de messagerie utilisent le chiffrement SSL/TLS (le « s » dans « https »), un adversaire qui surveille ton traffic réseau sait généralement quels sites web tu visites, mais pas ce que tu fais sur ces sites web. Si tu utilises Tor[15], un adversaire qui surveille ton traffic réseau sait que tu utilises Tor, mais pas quels sites web tu visites ni ce que tu fais sur ces sites web.

Tor est vulnérable aux attaques par corrélation, mais de telles attaques sont difficiles à mettre en oeuvre même pour des adversaires puissants. Les poursuites judiciaires contre le hacker anarchiste Jeremy Hammond sont un exemple d'une attaque par corrélation qui a fonctionné : les moments où le pseudonyme qu'il utilisait dans des salons de discussion était « en ligne » (obtenus par une analyse de son traffic réseau) ont été corrélés avec les moments où une opération de **surveillance physique (p. 47)** l'observait chez lui pour prouver que le pseudonyme lui appartenait[93].

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques, et en particulier utiliser Tor[15], pour que ce soit plus difficile pour un adversaire de surveiller et analyser ton traffic réseau.

Chiffrement (#2) : Tu peux chiffrer des données « en mouvement » pour que ce soit plus difficile pour un adversaire d'analyser ces données grâce à la science forensique appliquée aux réseaux informatiques.

Cloisonnement (#2) : Un adversaire peut établir des liens entre différentes identités numériques grâce aux empreintes laissées par leurs traffics réseau. Pour contrer ça, tu peux cloisonner différentes identités numériques en :

- Utilisant Tails[9] et en redémarrant entre chaque session.
- Utilisant Qubes OS[94] avec différentes machines virtuelles Whonix[95] que tu n'utilises pas simultanément.

[93]https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8

[94]https://qubes-os.org

[95]https://whonix.org

4.20. Surveillance physique

Utilisée par les tactiques : **Incrimination (p. 15)**

La surveillance physique est l'observation directe de personnes ou d'activités dans le but d'obtenir des informations. Une *opération de surveillance physique* est typiquement menée par une ou plusieurs *équipes de surveillance* composées d'individus ayant reçu une formation spécifique appelés des *opérateurs de surveillance*.

Parce qu'elle nécessite le déploiement d'opérateurs de surveillance sur le terrain, parfois pour de longues périodes, la surveillance physique est une méthode de surveillance coûteuse en ressources et en personnel.

4.20.1. Aérienne

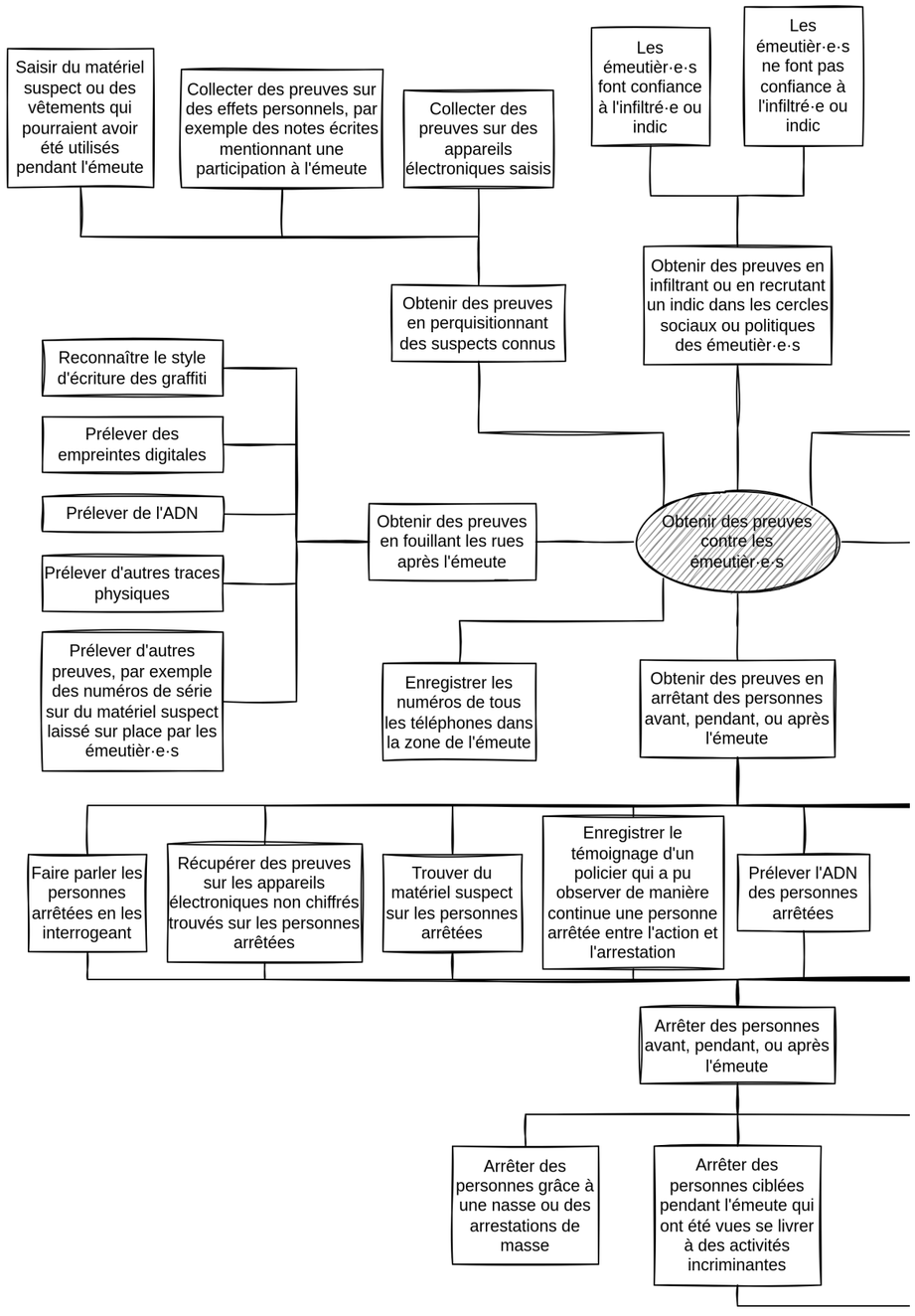
La surveillance physique aérienne est l'observation directe de personnes ou d'activités dans le but d'obtenir des informations. Dans de nombreux pays, les hélicoptères ont traditionnellement été le principal outil pour ce type de surveillance. Les drones devenant moins coûteux, leur utilisation devient plus courante. Les avions de surveillance sont aussi utilisés occasionnellement et sont bien plus discrets que les hélicoptères.

Voici des exemples de surveillance physique aérienne :

- Observer la foule pendant des manifestations ou rassemblements, souvent dans le cadre d'une opération de surveillance **visible (p. 50)**.
- Améliorer les chances de suivre la cible de la surveillance avec succès lors d'une opération de surveillance **cachée (p. 48)**, notamment de nuit.
- Localiser des suspects peu après qu'une action ait eu lieu et que l'adversaire ait été alerté, notamment dans des zones rurales ou de nuit (dans le cas d'un incendie volontaire en Allemagne, un hélicoptère de la police est intervenu en volant au-dessus de la zone la nuit de l'incendie[96]).
- Localiser des suspects dans le cadre de **patrouilles de police (p. 29)** de routine dans des zones où le risque d'activité criminelle est élevé.

Les avions de surveillance peuvent surveiller des villes entières, photographiant jusqu'à 80 kilomètres carrés par

[96]https://actforfree.noblogs.org/post/2023/11/13/munich-germany-geothermal-energy-gets-hot-and-not-only



(4) Arbre d'attaque « Émeute » (complet, partie gauche).

physique (p. 47) pour trouver les numéros de téléphone de personnes que Boris rencontrait—et ont ensuite identifié ces personnes en demandant aux opérateurs de téléphonie mobile les noms correspondant aux numéros de téléphone[22].

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont utilisé des IMSI-catchers pour identifier les numéros de téléphone de personnes qui vivaient dans des lieux en lien avec la lutte contre Cigéo ou qui participaient à des manifestations[13].

4.19.4. Malware

Un malware est un logiciel malveillant installé sur un appareil numérique comme un ordinateur, serveur, ou téléphone portable, pour compromettre l'appareil. Les malware peuvent faire beaucoup de choses différentes, mais contre les anarchistes et autres rebelles ils visent typiquement à surveiller l'appareil compromis à distance en prenant des captures d'écran et en enregistrant le texte entré sur l'appareil, et à pister la position de l'appareil (dans le cas des téléphones).

Un logiciel malveillant peut être installé sur un appareil :

- À distance, typiquement grâce au phishing[88] par email ou messages (SMS, etc.) Pour être efficace, le phishing nécessite souvent que la cible ouvre un fichier ou un lien malveillant.
- En **accédant physiquement (p. 43)** à l'appareil.

Voir le sujet « Logiciels malveillants ciblés »[89].

Mesures d'atténuation

Analyse des ordinateurs et téléphones (#2) : Tu peux faire une analyse des ordinateurs et téléphones pour détecter des traces de malware sur un appareil sur lequel un malware est ou a été installé.

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques, et en particulier utiliser des systèmes d'exploitation axés sur la sécurité pour que ce soit plus difficile pour un adversaire d'installer un malware sur tes appareils numériques.

Chiffrement (#2) : Tu peux chiffrer les données « en mouvement » pour que ce soit plus difficile pour un adversaire d'installer un malware via l'*injection de paquet réseau*, un vecteur d'installation pour certains malware, comme Pegasus[90].

Cloisonnement (#2) : Si un adversaire installe un malware sur une clé USB Tails[9] ou une machine virtuelle Qubes OS[91] que tu utilises pour des identités numériques différentes, il peut relier ensemble tes différentes identités. Pour contrer ça, tu peux utiliser différentes clés USB Tails ou machines virtuelles Qubes OS pour différentes identités numériques.

Opérations répressives

Scripta Manent (#2) : Un malware a été installé sur l'ordinateur d'un·e des accusé·e·s[92]. Le malware, qui a été installé à distance par Internet, a ciblé un ordinateur Windows et était capable d'enregistrer le texte tapé au clavier, de faire des captures d'écran régulières, et d'enregistrer les communications envoyées et reçues par l'ordinateur.

Répression du sabotage de l'usine Lafarge (#2) : Les enquêteurs ont fait cinq requêtes pour installer à distance des logiciels espions[18]. Parmi celles-ci, une installation a été fructueuse (sur un iPhone SE 2020) et leur a donné accès à une conversation de groupe Signal.

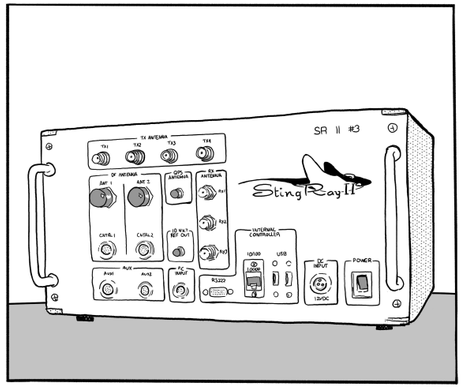
4.19.5. Science forensique appliquée aux réseaux informatiques

La science forensique appliquée aux réseaux informatiques est la surveillance et l'analyse de traffic réseau.

Les informations qui transitent sur les réseaux sont volatiles, conçues pour être transmises puis effacées, et les surveiller nécessite donc une approche proactive. De nombreux pays ont construit des centres d'analyse de données qui stockent des quantités énormes de données pendant des jours, des mois ou des années pour les analyser plus tard. Un adversaire peut aussi surveiller ton traffic réseau avec la **collaboration de ton fournisseur d'accès à Internet (p. 18)**, en compromettant ton routeur avec un **malware (p. 46)**, ou en surveillant tes connexions réseau filiaires ou sans fil à partir d'un véhicule de surveillance à proximité de ton domicile.

[88] https://fr.wikipedia.org/wiki/Hameçonnage
[89] https://notrace.how/resources/fr/#topic=targeted-malware
[90] https://forbiddenstories.org/fr/a-propos-du-projet-pegasus
[91] https://www.qubes-os.org
[92] https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy

4.19.3. IMSI-catcher



Un IMSI-catcher (aussi connu sous le nom de *Stingray*) est un appareil utilisé pour collecter des informations à propos de tous les téléphones allumés dans une zone restreinte (de quelques mètres à plusieurs centaines de mètres) autour de lui. Un IMSI-catcher passif écoute simplement le traffic, alors qu'un IMSI-catcher actif agit comme une « fausse » antenne téléphonique entre les téléphones et les vraies antennes téléphoniques.

Un IMSI-catcher peut collecter les informations suivantes à propos des téléphones autour de lui :

- Leurs numéros.
- Leurs numéros IMSI[86] et IMEI[20].
- Des données et métadonnées à propos de leur activité : le contenu des SMS et appels classiques, la liste des sites web visités, des métadonnées à propos de leur utilisation d'applications de messagerie chiffrées de bout-en-bout (par exemple, quand est-ce que Signal est utilisé et la taille approximative des messages envoyés ou reçus sur Signal).

Un adversaire peut utiliser un IMSI-catcher pour relier des personnes et des numéros de téléphone. Par exemple :

- Pendant une manifestation, pour enregistrer les numéros de téléphone de tous les téléphones présents à la manifestation et ensuite obtenir les noms associés à ces numéros de téléphone grâce à la **collaboration des opérateurs de téléphonie mobile (p. 19)**.
- Dans le cadre d'une opération de **surveillance physique (p. 47)** pour trouver le numéro de téléphone de la cible ou les numéros de téléphone des personnes en contact avec la cible.

Un adversaire peut aussi utiliser un IMSI-catcher pour enregistrer l'activité d'un téléphone. Par exemple :

- Pour enregistrer l'activité d'un téléphone cible sans avoir besoin de la collaboration de l'opérateur de téléphonie mobile (qui, dans certains contextes, peut nécessiter un mandat).
- Pour enregistrer l'activité d'un téléphone cible quand l'adversaire sait où le téléphone est utilisé, mais ne connaît pas son numéro.

Voir le sujet « IMSI-catchers »[87].

Mesures d'atténuation

Chiffrement (#2) : Tu peux chiffrer les données « en mouvement » d'un téléphone pour que si les données sont collectées par un IMSI-catcher, elles ne puissent pas être analysées. Par exemple, tu peux utiliser des applications de messagerie chiffrées de bout-en-bout plutôt que des SMS et appels classiques pour tes communications téléphoniques.

Recherche de dispositifs de surveillance (#2) : Tu peux faire une recherche de dispositifs de surveillance pour détecter la présence d'un IMSI-catcher.

Détecter la présence d'un IMSI-catcher peut avoir plusieurs avantages :

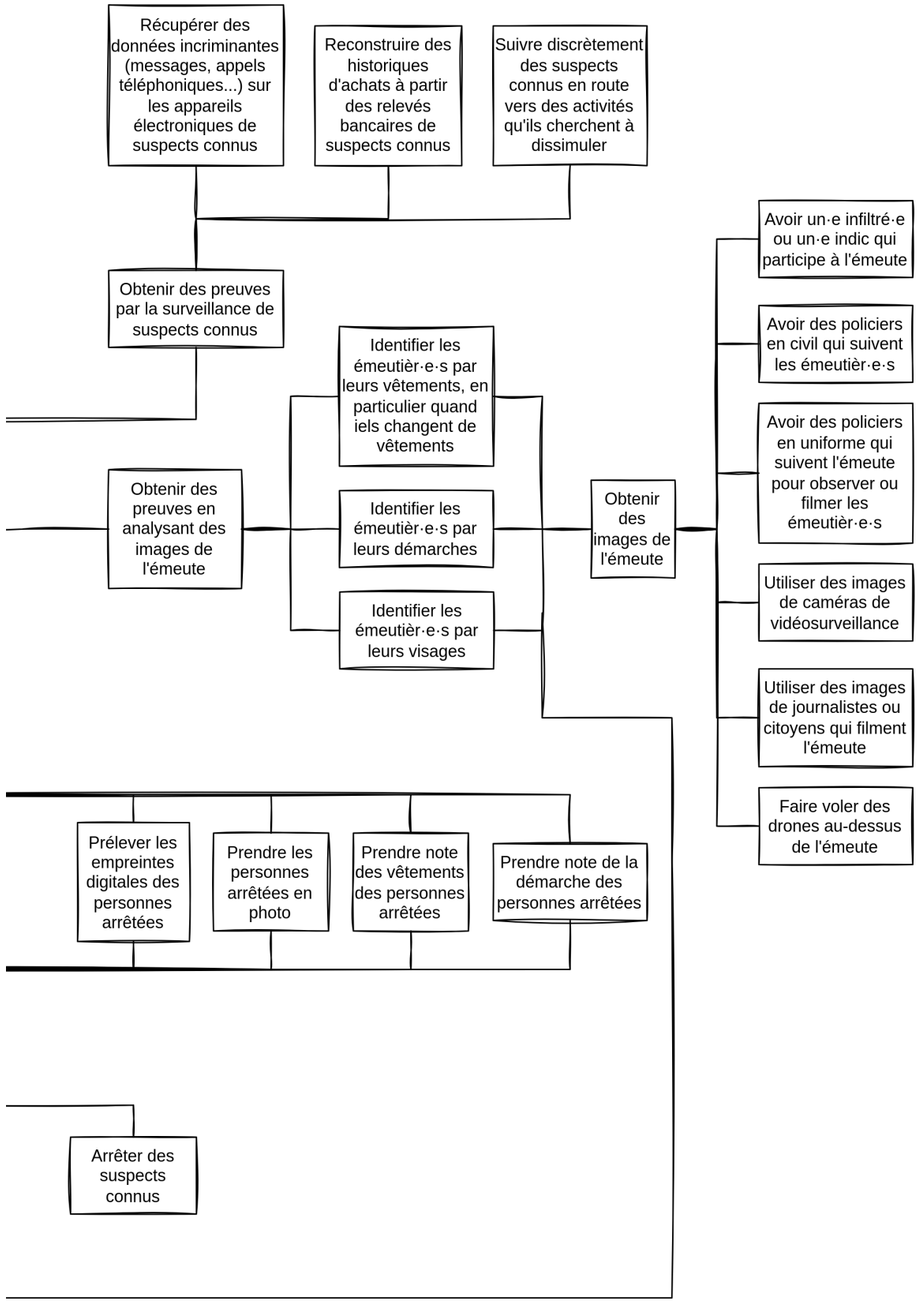
- La présence d'un IMSI-catcher est un bon indice du niveau de surveillance mis en place par un adversaire.
- Si l'IMSI-catcher est utilisé dans un évènement ou une manifestation, sa présence peut t'aider à convaincre les participant·e·s d'éteindre leurs téléphones.
- Tu peux détruire l'IMSI-catcher (les IMSI-catchers professionnels peuvent coûter très cher).

Opérations répressives

Opération contre Boris (#2) : Les enquêteurs ont utilisé des IMSI-catchers lors d'opérations de **surveillance**

[86] Un numéro International Mobile Subscriber Identity (IMSI, identité internationale d'abonné mobile) est un numéro qui identifie une carte SIM de manière unique.

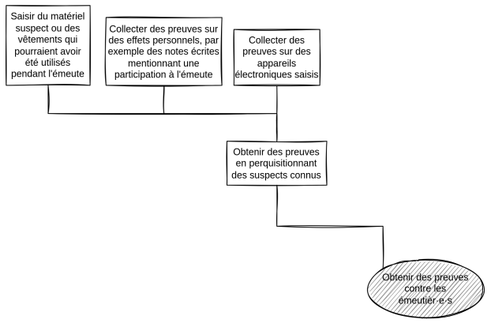
[87] https://notrace.how/resources/fr/#topic=imsi-catchers



(4) Arbre d'attaque « Émeute » (complet, partie droite).

2.2.2. Identifier les techniques

Vous identifiez toutes les techniques représentées sur l'arbre en associant les nœuds aux techniques de la Bibliothèque de menaces. Vous faites ça branche par branche pour éviter de vous perdre : c'est mieux de commencer par les nœuds les plus proches du nœud racine, puis de remonter la branche.



(5) Arbre d'attaque « Émeute » (branche perquisition).

Vous commencez avec la branche « Obtenir des preuves en perquisitionnant des suspects connus » (5) :

- « Obtenir des preuves en perquisitionnant des suspects connus » correspond à **Perquisition (p. 30)**.
- « Collecter des preuves sur des appareils électroniques saisis » correspond à **Surveillance numérique ciblée : Accès physique (p. 43)** parce qu'ils auraient besoin d'accéder à vos appareils électroniques, et à **Surveillance numérique ciblée : Contournement de l'authentification (p. 43)** si ils essaient de deviner vos mots de passe ou de casser le chiffrement.
- Les autres nœuds ne correspondent à rien, ils font juste partie de la perquisition.

À ce stade, ça peut être utile d'évaluer les risques des techniques que vous listez—ça vous aidera à décider quelles techniques vous voulez atténuer, et comment. Voir la section « Évaluer les risques », p. 13 sur comment évaluer les risques d'une technique en utilisant les concepts de *probabilité* et d'*impact*.

Ensuite vous passez à la branche suivante jusqu'à ce que tout l'arbre soit fait, en construisant un tableau (6).

Technique	Mesures d'atténuation	Implémentations
Perquisition (risque moyen)		
Accès physique (risque moyen)		
Contournement de l'authentification (risque faible)		

(6) Début du tableau.

2.2.3. Identifier les mesures d'atténuation

Ensuite, vous identifiez les mesures d'atténuation que vous voulez implémenter en regardant les mesures d'atténuation que la Bibliothèque de menaces suggère pour les techniques du tableau.

Pour la branche choisie pour cet exemple (5), vous décidez d'implémenter :

- Pour « Perquisition », **Se préparer à la répression (#2)**, **Se préparer aux perquisitions (#2)** et **Cachette ou planque (#2)**. Vous ne voulez pas implémenter **Clandestinité (#2)** parce que vous ne voulez pas entrer en clandestinité.
- Pour les deux techniques « Surveillance numérique ciblée », **Bonnes pratiques numériques (#2)** est la seule mesure d'atténuation qui a du sens dans votre contexte.

Vous mettez à jour le tableau (7).

- Brute force : deviner le mot de passe de chiffrement via des tentatives d'authentification automatiques et répétées.
- Compromettre l'appareil numérique avec un **malware (p. 46)** installé à distance ou en **accédant physiquement (p. 43)** à l'appareil.
- Exploiter une faille au niveau de l'implémentation du processus de chiffrement.

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques, et en particulier utiliser des systèmes d'exploitation axés sur la sécurité avec un chiffrement complet du disque et des mots de passe robustes, pour que ce soit plus difficile pour un adversaire de contourner l'authentification de tes appareils numériques. Par exemple :

- Sur des ordinateurs, tu peux utiliser le chiffrement complet du disque de Linux appelé LUKS, qui est utlisé par de nombreux systèmes Linux, dont Debian[82] et Tails[9], et que le service de police scientifique de la police fédérale allemande n'a pas pu déchiffrer après avoir essayé pendant une année[83].
- Sur des téléphones, tu peux utiliser GrapheneOS, dont le chiffrement complet du disque fait qu'il est plus difficile pour un adversaire de deviner le mot de passe de chiffrement par brute force : après 140 essais ratés, chaque essai est retardé d'un jour complet[84].

Mesures de détection d'accès physique (#2) : Tu peux prendre des mesures de détection d'accès physique pour détecter si un appareil a été **accédé physiquement (p. 43)**.

Une fois qu'un appareil a été accédé physiquement par un adversaire, tu devrais le considérer comme compromis et ne plus jamais t'authentifier dessus. En effet, dans le pire des cas, l'adversaire pourrait avoir copié les données de l'appareil et avoir compromis son firmware de telle sorte que quand tu entres ton mot de passe, il peut l'obtenir à distance et l'utiliser pour déchiffrer les données.

[82] https://debian.org
[83] https://notrace.how/resources/fr/#parkbank
[84] https://grapheneos.org/faq#encryption

Recherche de dispositifs de surveillance (#2) : Avant d'entrer un mot de passe dans une pièce où des **dispositifs de surveillance cachés vidéo (p. 24)** pourraient être présents, tu peux faire une recherche de dispositifs de surveillance pour localiser de tels dispositifs et les retirer.

Opérations répressives

Répression contre Zündlumpen (#2) : Dans certaines des perquisitions d'avril 2022, les policiers ont saisi des smartphones immédiatement après être entrés et les ont branchés à des batteries externes, vraisemblablement pour les empêcher de s'éteindre, ce qui aurait ré-activé leur chiffrement[85].

Répression du sabotage de l'usine Lafarge (#2) : Les enquêteurs ont saisi plusieurs smartphones chiffrés dans les perquisitions et ont tenté d'accéder à leurs données chiffrées, avec plus ou moins de succès en fonction des téléphones[18] :

- Pour les iPhones qui ont été saisis allumés, ils ont exploité les failles de sécurité qui existent quand ils sont allumés pour contourner leur chiffrement et accéder aux données chiffrées.
- Pour tous les téléphones Android (qu'ils aient été saisis allumés ou éteints) et pour un iPhone saisi éteint, ils ont extrait les partitions chiffrées des téléphones et ont tenté de deviner leurs mots de passe par *brute force* depuis un ordinateur.

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont contourné l'authentification de cinq supports de stockage chiffrés trouvés dans des perquisitions[13] :

- Un disque dur grâce au mot de passe très simple « stopcigeo », qu'ils ont peut-être deviné.
- Un disque dur grâce à un mot de passe trouvé sur un post-it sous l'ordinateur contenant le disque dur.
- Un disque dur grâce à un mot de passe qui leur a été donné par le/la propriétaire de l'ordinateur contenant le disque dur.
- Deux disques durs grâce à des mots de passe qu'ils ont trouvé dans un document texte sur un disque dur préalablement déchiffré.

[85] https://zuendlappen.noblogs.org/post/2022/05/07/muenchen-ueber-razzien-und-ein-%c2%a7129-verfahren-gegen-anarchistinnen-und-den-raub-einer-druckerei

ici sur les techniques qui ont plus de chances d'être utilisées contre des anarchistes et autres rebelles.

Voir le sujet « Surveillance numérique »[73].

4.19.1. Accès physique

L'accès physique est le processus par lequel un adversaire accède physiquement à un appareil électronique afin d'accéder à ses données ou de le compromettre.

Voici des exemples notables d'appareils électroniques auxquels un adversaire peut accéder physiquement :

- Des ordinateurs, téléphones, et supports de stockage (par exemple des disques dur, clés USB, cartes SD).
- Des imprimantes, appareils photos, télévisions « intelligentes ».
- Des véhicules. Par exemple, les systèmes embarqués[80] des véhicules modernes peuvent stocker l'historique des positions du véhicule.

Si un adversaire accède physiquement à un appareil, il peut :

- Lire les données non chiffrées de l'appareil, ou ses données chiffrées si il est allumé (et donc que son **chiffrement (#2)** n'est pas efficace).
- Compromettre l'appareil avec un **malware (p. 46)**.
- Compromettre l'appareil avec un enregistreur de frappes matériel[81].

Un adversaire peut accéder physiquement à un appareil :

- Pendant une **perquisition (p. 30)** ou une **visite discrète de domicile (p. 53)**.
- Après t'avoir arrêté si tu as l'appareil sur toi.
- Pendant un contrôle aux frontières.
- Via un·e **infiltré·e (p. 27)** ou un·e **indic (p. 26)** qui a accès à l'appareil.

Mesures d'atténuation

Analyse des ordinateurs et téléphones (#2) : Tu peux faire une analyse des ordinateurs et téléphones pour détecter si un appareil a été accédé physiquement par un adversaire.

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques pour contrer le risque qu'un adversaire accède physiquement à tes appareils numériques. Par exemple, si tu vas à un évènement ou une manifestation et que tu penses que tu pourrais être arrêté·e, tu ne devrais pas prendre ton téléphone avec toi.

Dessiner une carte de son réseau (#2) : Un adversaire pourrait accéder physiquement à tes appareils numériques via un·e **infiltré·e (p. 27)** ou un·e **indic (p. 26)**. Pour contrer ça, tu peux dessiner une carte de ton réseau pour t'aider à identifier les personnes en qui tu fais assez confiance pour les laisser accéder à tes appareils numériques.

Détection d'intrusion physique (#2) : Tu peux prendre des mesures de détection d'intrusion physique pour détecter quand un espace a été accédé physiquement par un adversaire.

Mesures de détection d'accès physique (#2) : Tu peux prendre des mesures de détection d'accès physique pour détecter quand quelque chose a été accédé physiquement par un adversaire.

4.19.2. Contournement de l'authentification

Le contournement de l'authentification est le processus par lequel un adversaire contourne le **chiffrement complet du disque (#2)** qui protège l'accès à un appareil numérique. Un adversaire peut contourner l'authentification grâce à des erreurs humaines, des mots de passe faibles, ou des failles techniques.

Un adversaire peut contourner l'authentification des manières suivantes :

- Accéder à un appareil alors qu'il est allumé (et donc que son chiffrement n'est pas efficace).
- Trouver le mot de passe de chiffrement écrit quelque part.
- Forcer le propriétaire de l'appareil à fournir le mot de passe de chiffrement en utilisant des **techniques d'interrogatoire (p. 51)**, y compris, dans certains contextes, de la **violence physique (p. 53)**.
- Interception visuelle : observer le propriétaire de l'appareil taper le mot de passe de chiffrement via une **caméra cachée (p. 24)** ou un·e **infiltré·e (p. 27)** ou **indic (p. 26)**.

[80] https://fr.wikipedia.org/wiki/Système_embarqué_mobile
[81] https://en.wikipedia.org/wiki/Hardware_keylogger

Technique	Mesures d'atténuation	Implémentations
Perquisition (risque moyen)	Se préparer à la répression Se préparer aux perquisitions Cachette ou planque	
Accès physique (risque moyen)	Bonnes pratiques numériques	
Contournement de l'authentification (risque faible)	Bonnes pratiques numériques	

(7) Début du tableau, avec les mesures d'atténuation.

2.2.4. Décider comment implémenter les mesures d'atténuation

Enfin, vous décidez comment implémenter les mesures d'atténuation du tableau. Lire leurs entrées dans la Bibliothèque de menaces peut vous donner des idées. Le risque évalué pour chaque technique vous aide à savoir quels efforts mettre dans les mesures d'atténuation. Vous décidez des implémentations suivantes :

- « Se préparer à la répression » : Comme toi et tes camarades vivez tou·te·s au même endroit, il y a un risque que vous soyez tou·te·s arrêté·e·s après une perquisition. Vous allez vous assurer que d'autres camarades sachent comment vous soutenir si cela se produit.
- « Se préparer aux perquisitions » : Vous décidez d'arrêter de stocker les feux d'artifices sous ton lit.
- « Cachette ou planque » : Vous décidez d'enterrer un contenant hermétique dans une forêt proche pour stocker les feux d'artifice. Quand l'un·e d'entre vous y accède, iel doit porter des gants et s'assurer qu'il n'y a personne à proximité.
- « Bonnes pratiques numériques » : Vos appareils sont déjà chiffrés, et de toute façon vous ne les utilisez pas pour parler des émeutes. Vous devez vous renseigner pour savoir si le chiffrement d'un téléphone fonctionne quand il est allumé et verrouillé parce que vous n'êtes pas sûr·e·s.

À ce stade, ça peut être utile de ré-évaluer les risques des techniques pour vous assurer qu'ils ont été suffisamment réduits par les mesures d'atténuation que vous avez décidé d'implémenter.

Vous mettez à jour le tableau (8).

Technique	Mesures d'atténuation	Implémentations
Perquisition (risque ~~moyen~~) FAIBLE	Se préparer à la répression Se préparer aux perquisitions Cachette ou planque	S'assurer que d'autres camarades savent quoi faire en cas de perquisition : prévenir des avocats etc. Arrêter de stocker les feux d'artifice sous le lit !! Boîte dans la forêt pour les feux d'artifice (gants ! s'assurer qu'il y a personne autour !)
Accès physique (risque ~~moyen~~) FAIBLE	Bonnes pratiques numériques	Ne pas parler de l'émeute au téléphone ! Rechercher : est-ce que le chiffrement d'un téléphone fonctionne s'il est allumé et verrouillé ?
Contournement de l'authentification (risque faible)	Bonnes pratiques numériques	(pareil qu'au dessus)

(8) Début du tableau, avec les mesures d'atténuation et leurs implémentations.

2.2.5. Brûler ou numériser vos notes

Les notes prises pendant cet exercice ne devraient pas être conservées telles quelles parce qu'elles pourraient être considérées comme preuves d'une conspiration. Tu as deux options :

1. À la fin de l'exercice, tu mémorises les notes et tu les brûles. Avec cette approche, c'est difficile de reprendre les notes plus tard pour les retravailler.
2. À la fin de l'exercice, tu numérises les notes en les retapant manuellement sur une clé USB chiffrée avec Tails[9] (n'oublie pas d'adopter de **bonnes pratiques numériques (#2)**). Tu peux utiliser Libreoffice Draw (inclus dans Tails par défaut) pour dessiner l'arbre d'attaque. Une fois les notes numérisées, elles ne devraient pas être imprimées parce que cela pourrait laisser des traces sur l'imprimante, mais elles peuvent être de nouveau copiées manuellement sur papier pour pouvoir les relire loin des écrans.

[9] https://tails.net/index.fr.html

2.2.6. Débriefing de l'action

Après l'émeute, toi et tes camarades prenez du temps pour faire un débriefing de l'action : dans des **conversations en extérieur et sans appareils (#2)**, vous discutez de ce qui s'est bien ou mal passé, et de si vous pouvez améliorer votre arbre d'attaque ou la manière dont vous avez implémenté les mesures d'atténuation.

2.3. Évaluer les risques

Le risque est la combinaison de l'impact et de la probabilité d'une technique. Si une technique aurait un fort impact, mais qu'il est très peu probable qu'elle soit utilisée, elle pourrait être considérée comme peu risquée. Si une technique aurait un impact moyen, mais qu'il est probable qu'elle soit utilisée, elle pourrait être considérée comme très risquée. Si tu considères qu'une technique est risquée, cela veut dire que tu devrais mettre plus d'efforts dans les mesures d'atténuation que tu prends pour cette technique.

Par exemple, dans la plupart des contextes, si tu prévois de commettre un incendie volontaire, la technique **Science forensique : ADN (p. 31)** est très risquée. En effet, elle a un fort impact (une correspondance ADN avec la scène de crime d'un incendie volontaire est une preuve solide dans un procès) et une forte probabilité (dans la plupart des contextes, des analyses ADN sont systématiquement réalisées dans les enquêtes sur des incendies volontaires).

2.3.1. Impact

L'impact est une mesure des conséquences de l'utilisation d'une technique. Il dépend de la tactique :

- Tactique « dissuasion » : L'impact dépend de si la cible est dissuadée avec succès.
- Tactique « incrimination » : L'impact dépend de la « solidité » des preuves collectées.
- Tactique « arrestation » : L'impact dépend de si la cible est appréhendée avec succès.

2.3.2. Probabilité

La probabilité est une mesure d'à quel point il est probable qu'un adversaire tente d'utiliser une technique.

2.3.3. Les ressources de l'adversaire augmentent le risque

Si plus de ressources sont dévouées à la répression d'une action, il peut être plus probable qu'une technique donnée soit utilisée, augmentant sa *probabilité*, et elle peut être utilisée plus minutieusement, augmentant son potentiel *impact*. De manière générale, un adversaire dévoue plus de ressources à la répression d'une action s'il se sent plus menacé par celle-ci.

Par exemple :

- Dans la plupart des contextes, des analyses ADN sont systématiquement réalisées dans les enquêtes sur des incendies volontaires. Si l'adversaire a des ressources limitées, les prélèvements peuvent être limités à des surfaces évidentes comme des poignées de porte. Si l'adversaire a plus de ressources—ce qui peut être le cas si l'incendie a causé beaucoup de dégâts—il est plus probable que la scène de crime soit fouillée en profondeur pour y trouver des preuves ADN.
- Dans la plupart des contextes, si l'adversaire est l'État, des actions classifiées comme « terrorisme » ou « menaces à la sécurité nationale » vont recevoir des quantités extraordinaires de ressources. L'État peut dévouer beaucoup de ressources à des actions qui ont eu lieu pendant un soulèvement, parce que le soulèvement a été perçu comme une menace à son intégrité.

2.3.4. Les mesures d'atténuation réduisent le risque

En prenant des mesures d'atténuation appropriées, tu deviens moins vulnérable à une technique, réduisant son potentiel *impact*.

Par exemple, tu es vulnérable aux analyses ADN parce que de l'ADN tombe en continu de ton corps. Si tu appliques des **protocoles de minimisation de l'ADN (#2)** en commettant un incendie volontaire, tu deviens moins vulnérable aux analyses ADN.

des images de vidéosurveillance, surtout si ses caractéristiques particulières sont minimisées. Par exemple, tu peux utiliser un vélo volé différent pour chaque action que tu fais.

Reconnaissance (#2) : Avant une action, tu peux identifier les positions des caméras de surveillance sur le lieu de l'action et prévoir de les éviter si possible.

Tenue anonyme (#2) : Tu peux porter une tenue anonyme pour empêcher un adversaire de t'identifier sur des images de vidéosurveillance.

Opérations répressives

Opération contre Boris (#2) : Peu après le sabotage d'avril, les enquêteurs ont récupéré les images de vidéosurveillance de commerces et de caméras municipales, et les listes de véhicules filmés par des systèmes de lecture automatisée de plaques d'immatriculation (LAPI) et des radars automatiques, tout ça dans un périmètre étendu autour du lieu du sabotage.

Opération de 2019-2020 contre Mónica et Francisco (#2) : Des images de vidéosurveillance publique ont été amplement utilisées par les enquêteurs pour reconstruire les déplacements de Mónica et Francisco avant et durant les actions, malgré les mesures d'atténuation qu'iels ont prises (prendre des taxis, changer de vêtements, porter des déguisements)[46].

Répression du sabotage de l'usine Lafarge (#2) : Immédiatement après l'action, les enquêteurs ont obtenu les images de vidéosurveillance de transports en commun (bus, gares, etc.), de commerces, de caméras de surveillance de maisons privées et de caméras municipales, le tout dans un périmètre étendu autour du lieu de l'action[18]. Les images de l'intérieur des bus semblent notamment avoir aidé à identifier des personnes qui s'étaient déplacées vers et depuis le lieu de l'action[56]. Les enquêteurs ont aussi obtenu les images de péages d'autoroute, vraisemblablement pour identifier les personnes à l'intérieur de voitures suspectées d'avoir emprunté l'autoroute vers ou depuis le lieu de l'action.

Prometeo (#2) : Deux des personnes ont prétendument été vues sur des images de vidéosurveillance quitter un magasin où les enquêteurs pensent que les enveloppes utilisées pour préparer les colis piégés ont été achetées[36].

Opération de 2013 contre Mónica et Francisco (#2) : Des images de vidéosurveillance publique ont été utilisées pour reconstruire les déplacements de Mónica et Francisco avant et après l'action[50]. Cela a montré qu'iels étaient près du lieu de l'action peu avant l'explosion de l'engin.

Opération contre Peppy et Krystal (#2) : Des images de vidéosurveillance d'un bus ont permis aux enquêteurs d'identifier la plaque d'immatriculation de la moto sur laquelle Peppy et Krystal sont arrivés au lieu de la manifestation et en sont partis[19].

Répression du premier incendie de Jane's Revenge (#2) : Des images de vidéosurveillance ont aidé à identifier un véhicule conduit par la personne, lorsqu'elle a été vue entrer dans un parking à pied après une manifestation, et que le véhicule a été vu quitter ce même parking quelques minutes plus tard[58].

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont utilisé des images des manifestations, filmées par des caméras de surveillance ou des policiers, pour[13] :

- Identifier une personne qui n'était que partiellement masquée, avec ses yeux, ses lunettes et son front visibles.
- Faire le lien entre une personne qui avait l'air enceinte au vu de son ventre, vue dans une manifestation, et une personne qui a accouché quelques mois plus tard.

Les trois du banc public (#2) : Dans la soirée précédant l'arrestation, une des personnes—alors qu'elle était suivie par des policiers—s'est arrêtée à une station-service et a été vue par les caméras de vidéosurveillance de la station acheter de l'essence et remplir un bidon d'essence[78]. Les policiers ont obtenu les images de vidéosurveillance le matin suivant.

4.19. Surveillance numérique ciblée

Utilisée par les tactiques : **Incrimination (p. 15)**

La surveillance numérique ciblée est la collecte et l'analyse ciblées de données et communications numériques.

Des techniques extrêmement avancées existent[79] dans l'arsenal des acteurs étatiques, mais on va se concentrer

[78] https://notrace.how/resources/fr/#parkbank

[79] https://anonymousplanet.org/guide.html#some-advanced-targeted-techniques

part pour des raisons mûrement réfléchies (par exemple écrire et envoyer un communiqué de revendication tout en adoptant de **bonnes pratiques numériques (#2)**).

4.18.4. Vidéosurveillance

La vidéosurveillance de masse est la collecte, le stockage, et l'analyse à grande échelle des données vidéo et audio de caméras de vidéosurveillance. La vidéosurveillance de masse vise à capturer l'identité des personnes qui traversent un espace et à étendre sa couverture autant que possible. Certains pays ont désormais plus de caméras de vidéosurveillance que d'habitants.

Collecte

Voici des sources d'images de vidéosurveillance :

- Les caméras dans la rue ou autres espaces publics.
- Les caméras dans des bâtiments privés (par exemple des magasins, des bureaux).
- Les caméras dans les transports en commun comme les bus, les trains, les autoroutes, etc.
- Les caméras-sonnettes comme Amazon Ring.
- Les caméras intégrées à des véhicules comme sur les Tesla.

Les caméras de vidéosurveillance peuvent grandement varier en qualité, portée, capacités à voir la nuit, présence de microphones, etc.

Stockage

Après avoir été collectées, les images de vidéosurveillance sont souvent stockées pendant un certain temps (de quelques jours à des durées indéfinies) avant d'être effacées.

Analyse

Un adversaire peut analyser des images de vidéosurveillance :

- En temps réel si les caméras sont intégrées à un réseau centralisé. L'analyse en temps réel peut avoir lieu soit dans le cadre d'une surveillance de routine soit pour des évènements spéciaux (comme des manifestations).
- Rétroactivement si les images de vidéosurveillance ont été stockées. L'analyse rétroactive peut aider à identifier un suspect grâce à son **visage (p. 38)**, sa **démarche (p. 38)**, sa **voix (p. 36)**, etc.

L'analyse d'images de vidéosurveillance peut être faite :

- Par des humains.
- Par des systèmes automatisés comme les systèmes de lecture automatisée de plaques d'immatriculation ou les **systèmes de reconnaissance faciale (p. 38)**.

Voir aussi

- Pas vue pas prise: contre la vidéo-surveillance[74].
- Les sujets « Vidéosurveillance[75] » et « Lecteurs de plaques d'immatriculation automatisés[76] ».

Mesures d'atténuation

Achats anonymes (#2) : Tu peux faire des achats anonymes pour empêcher un adversaire de t'identifier sur les images de vidéosurveillance de magasins physiques.

Attaque (#2) : Tu peux mettre hors d'usage[77] des caméras de surveillance.

Conversations en extérieur et sans appareils (#2) : Tu peux avoir des conversations sensibles loin de caméras de surveillance pour empêcher un adversaire d'enregistrer ces conversations avec des caméras de surveillance équipées de microphones.

Dissimulation biométrique (#2) : Si tu es filmé·e par des caméras de surveillance, tu peux :

- Pour contrer la **reconnaissance de démarche (p. 38)**, porter des vêtements amples qui cachent la forme de ton corps, utiliser un parapluie ou d'autres objets couvrants, ou changer drastiquement ton style de marche en adoptant une « démarche bizarre ».
- Pour contrer la **reconnaissance faciale (p. 38)**, porter un masque qui cache les caractéristiques de ton visage, et des lunettes de soleil ou un chapeau à bord bas pour couvrir tes yeux.

Déplacement en vélo (#2) : Tu peux utiliser un vélo plutôt qu'un autre type de véhicule : comparé aux autres véhicules, un vélo est beaucoup plus difficile à identifier sur

[74] https://notrace.how/resources/fr/#pas-vue
[75] https://notrace.how/resources/fr/#topic=video-surveillance
[76] https://notrace.how/resources/fr/#topic=automated-license-plate-readers
[77] https://notrace.how/resources/fr/#detruisons-les-cameras

2.3.5. Risque et contexte local

Comprendre les habitudes et motivations d'un adversaire dans la répression d'une action peut t'aider à identifier le panel de techniques répressives qu'il utilisera probablement, et avec quelle minutie il les utilisera. Les **opérations répressives (#2)** peuvent t'aider à comprendre comment une technique donnée est utilisée dans un contexte donné.

2.4. Conseils supplémentaires pour utiliser la Bibliothèque de menaces

La page d'accueil[5] de la Bibliothèque de menaces présente une vue d'ensemble de toutes les tactiques et techniques, ainsi que des boutons qui te permettent de cacher ou d'afficher des techniques spécifiques. Par exemple, tu peux vouloir afficher seulement les techniques qui correspondent à ton modèle de menace pour mieux les visualiser. Si tu suis le processus que nous proposons ci-dessus et que tu dessines ton propre arbre d'attaque, la vue d'ensemble peut t'aider à penser à des techniques pertinentes qui manquent à ton arbre.

La Bibliothèque de menaces accepte les contributions externes, comme :

- Proposer des modifications à apporter à des techniques, mesures d'atténuation ou opérations répressives existantes.
- Suggérer l'ajout de nouvelles techniques, mesures d'atténuation ou opérations répressives.
- Des arbres d'attaque pour différents types de projets.
- Traduire la Bibliothèque de menaces dans de nouvelles langues.

Voir la **section « Contribuer » (#2)** pour plus d'informations.

3. Tactiques

3.1. Dissuasion

Utilise les techniques :

Augmentation de la présence policière (p. 16)
Doxing (p. 25)
Frapper aux portes (p. 25)
Patrouilles de police (p. 29)
Surveillance de masse (p. 39)
Violence physique (p. 53)

Dans certains contextes, en plus ou à la place d'autres tactiques un adversaire peut tenter de t'empêcher ou te décourager d'atteindre tes objectifs. Cela peut être parce qu'il est incapable ou réticent à t'incriminer ou t'arrêter, ou parce qu'il pense que te décourager est une bonne stratégie complémentaire. On appelle ce processus *dissuasion*.

3.2. Incrimination

Utilise les techniques :

Cartographie de réseau (p. 16)
Chiens de détection (p. 17)
Collaboration des fournisseurs de service (p. 17)
Construction parallèle (p. 20)
Coopération internationale (p. 21)
Dispositifs de surveillance cachés (p. 21)
Fabrication de preuves (p. 25)
Frapper aux portes (p. 25)
Indics (p. 26)
Infiltré·e·s (p. 27)
Interprétation biaisée des preuves (p. 28)
Open-source intelligence (p. 28)
Patrouilles de police (p. 29)
Perquisition (p. 30)
Science forensique (p. 31)
Surveillance de masse (p. 39)
Surveillance numérique ciblée (p. 42)
Surveillance physique (p. 47)
Techniques d'interrogatoire (p. 51)
Violence physique (p. 53)
Visite discrète de domicile (p. 53)
Vérifications d'identité (p. 52)

Afin de t'arrêter et de te retirer de la société—généralement par l'emprisonnement—un adversaire peut avoir besoin de convaincre un juge de ta participation à des activités illégales. Dans ce but, les autorités compétentes vont tenter de trouver des preuves de ces activités. En fonction du contexte et des personnes impliquées, les juges peuvent être plus ou moins faciles à convaincre. On appelle ce processus *incrimination*.

3.3. Arrestation

Utilise les techniques :

Augmentation de la présence policière (p. 16)
Chiens de détection (p. 17)
Coopération internationale (p. 21)
Patrouilles de police (p. 29)
Perquisition (p. 30)
Systèmes d'alarme (p. 50)
Vigiles (p. 52)
Vérifications d'identité (p. 52)

Afin de te retirer de la société—généralement par l'emprisonnement—un adversaire doit pouvoir te localiser physiquement et t'arrêter.

Mesures d'atténuation

Attaque (#2) : Si un civil te suit après une action, tu peux lui faire peur avec des menaces ou du spray au poivre. Si un civil essaie d'appeler la police, tu peux détruire son téléphone.

Préparation minutieuse de l'action (#2) : Les civils peuvent t'observer pendant une action et transmettre leurs observations à un adversaire. Pour contrer ça, tu peux mener les actions la nuit ou dans des zones peu fréquentées pour minimiser les témoins, et utiliser un·e guetteu·r·se pour être avertit de la présence de témoins dès qu'ils sont repérés. Fais attention aux balcons et fenêtres surplombant le lieu de l'action.

Tenue anonyme (#2) : Tu peux porter une tenue anonyme pour empêcher les civils de fournir une description de toi qui serait utile à un adversaire.

Opérations répressives

Fenix (#2) : Quand Lukáš Borl était en clandestinité, sa photo et ses informations personnelles ont été publiées sur le site web de la police nationale pour encourager les citoyens à envoyer à la police des informations à son propos[72].

Opération de 2019-2020 contre Mónica et Francisco (#2) : La vendeuse du magasin de téléphones portables où Mónica a acheté un téléphone qui a été utilisé dans l'action de 2020, interrogée par les enquêteurs, a donné une description d'une personne qui, selon les enquêteurs, correspondait à Mónica[46].

Partisans anarchistes biélorusses (#2) : En tentant de traverser la frontière entre la Biélorussie et l'Ukraine, les personnes se sont arrêtées à un magasin à environ 10 kilomètres de la frontière[13]. Un·e employé·e les a dénoncé aux gardes-frontière, ce qui a directement mené à leur arrestation.

4.18.3. Surveillance numérique de masse

[72] https://antifenix.noblogs.org/post/2016/03/11/confirmed-lukas-borl-under-police-investigation

Le Utah Data Center (UDC), un centre de stockage de données géant dans l'Utah, aux États-Unis, utilisé pour des activités de surveillance numérique de masse par les agences de renseignement des États-Unis.

La surveillance numérique de masse est la collecte, le stockage, et l'analyse à grande échelle des communications numériques de la totalité ou d'une partie substantielle d'une population.

La surveillance numérique de masse repose sur la collecte de données depuis diverses sources : transactions financières, contrôles aux frontières, pistage GPS des smartphones, et même lampadaires « intelligents ». Les avancées technologiques en capacité de stockage permettent à de vastes quantités de données d'être stockées dans des centres de stockage gérés par l'État. Les avancées technologiques en puissance de calcul permettent l'analyse automatique de ces données pour faciliter le travail des agences de police et de renseignement à l'échelle mondiale.

Voir le sujet « Surveillance numérique »[73].

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques pour rendre la surveillance numérique de masse inefficace. Par exemple, tu peux utiliser Tor[15] pour anonymiser tes activités Internet et tu peux utiliser des systèmes d'exploitation axés sur la sécurité et des applications qui limitent les données qu'elles stockent ou collectent à propos de toi.

Chiffrement (#2) : Tu peux chiffrer des données « en mouvement » pour empêcher des observateurs à certains endroits du réseau d'analyser ces données.

Éviter l'auto-incrimination (#2) : Un adversaire peut utiliser la surveillance numérique de masse pour extraire des informations auto-incriminantes d'un appareil numérique. Pour contrer ça, tu peux éviter de stocker de telles informations sur des appareils numériques à

[73] https://notrace.how/resources/fr/#topic=digital-surveillance

Mesures d'atténuation

Dissimulation biométrique (#2) : Tu peux porter un masque qui cache les caractéristiques de ton visage, et des lunettes de soleil ou un chapeau à bord bas pour couvrir tes yeux.

Tenue anonyme (#2) : Tu peux porter un masque qui couvre correctement ton visage, y compris tes sourcils et jusqu'en haut de ton nez.

Opérations répressives

Opération de 2019-2020 contre Mónica et Francisco (#2) : Pour identifier Mónica et Francisco sur les images de vidéosurveillance publique, des photos des deux ont été comparées aux images, avec une comparaison de plusieurs caractéristiques du visage : distance entre les yeux, rides, cicatrices de piercing, taille des oreilles, formes de la bouche et du nez[46].

Opération de 2013 contre Mónica et Francisco (#2) : La principale preuve contre Mónica et Francisco était une comparaison de photos des deux avec des images de vidéosurveillance publique qui montraient leurs visages découverts alors qu'iels étaient dans le métro, peu avant ou après l'action[50].

4.18. Surveillance de masse

Utilisée par les tactiques : **Dissuasion (p. 15)**, **Incrimination (p. 15)**

La surveillance de masse est la surveillance à grande échelle de la totalité ou d'une partie substantielle d'une population. C'est la surveillance de fond de notre société.

4.18.1. Fichiers de police

Les fichiers de police sont des dossiers physiques ou numériques produits par des agences de maintien de l'ordre. Les fichiers de police contiennent de grandes quantités d'informations à propos de beaucoup de choses, sont conservés indéfiniment ou pour de longues périodes, et peuvent être efficacement analysés et croisés grâce à des outils numériques.

Voici des exemples notables de fichiers de police :

- Les bases de données de documents d'identité officiels (cartes d'identité, permis de conduire, passeports).
- Les bases de données d'informations biométriques (photos de visages, empreintes digitales, ADN).
- L'historique des **vérifications d'identité (p. 52)**, amendes, arrestations, enquêtes, procédures judiciaires, et condamnations.

Mesures d'atténuation

Attaque (#2) : Tu peux détruire les armoires qui stockent les fichiers de police papier et les data centers qui stockent les fichiers de police numériques.

Opérations répressives

Opération contre Boris (#2) : Les enquêteurs ont découvert que l'ADN sur le bouchon de bouteille appartenait à Boris car son ADN était présent dans le Fichier national automatisé des empreintes génétiques (FNAEG)[22].

Les enquêteurs ont obtenu et analysé l'historique de l'activité de la police locale (contrôles d'identité et amendes) peu de temps avant et après les sabotages, dans différents périmètres autour de là où les sabotages ont eu lieu, en espérant vraisemblablement trouver les noms des saboteurs dans cet historique.

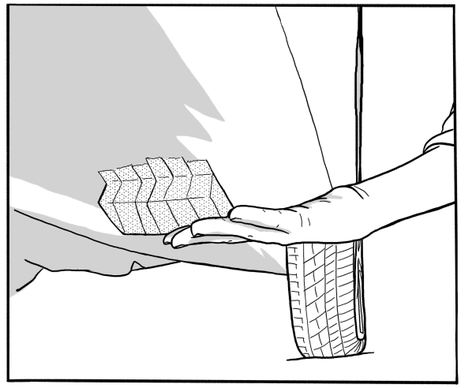
Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont amplement utilisé des fichiers de police pour faire des liens entre des gens, dont le Fichier national des permis de conduire, le Fichier des véhicules assurés, ainsi que les fichiers d'arrestations, de procédures judiciaires et de condamnations[13].

4.18.2. Mouchards civils

Les mouchards civils sont des personnes qui ne font pas partie des forces de sécurité d'un adversaire, mais qui préviendraient l'adversaire s'ils observaient quelque chose de suspect.

Par exemple, un mouchard civil qui est témoin d'un crime et qui s'identifie à l'État va probablement appeler la police, fournir une description du ou des suspects, et pourrait même suivre les suspects jusqu'à ce que la police intervienne ou témoigner dans le cadre d'une enquête criminelle.

4. Techniques



4.1. Augmentation de la présence policière

Utilisée par les tactiques : **Arrestation (p. 15)**, **Dissuasion (p. 15)**

L'augmentation de la présence policière est le processus par lequel la police augmente sa présence dans un endroit et à un moment donné pour deux raisons : pour intimider, et pour pouvoir intervenir plus facilement et plus rapidement.

Voici des exemples d'augmentation de la présence policière :

- Des **patrouilles de police (p. 29)** plus fréquentes dans une zone donnée.
- Le déploiement de policiers et de véhicules lors d'une manifestation. Dans les heures précédant une manifestation, des policiers et des véhicules peuvent se rassembler dans les rues autour de la manifestation ou autour de ses cibles présumées. Ce rassemblement peut leur donner l'opportunité de faire de la **surveillance visible (p. 50)** avant, pendant et après la manifestation.

Mesures d'atténuation

Attaque (#2) : Si tu t'attends à ce que la police augmente sa présence lors d'une manifestation, tu peux t'organiser pour t'assurer que la foule soit suffisamment nombreuse et féroce : les forces décentralisées et autonomes sont plus agiles que la chaîne de commandement rigide utilisée par le maintien de l'ordre pour le contrôle des foules. Par exemple, malgré des années de préparation pour militariser Hambourg, en Allemagne, pour le sommet du G20, des émeutièr·e·s ont été capables de libérer un quartier de l'occupation policière pendant toute une nuit[10].

Préparation minutieuse de l'action (#2) : Tu peux préparer minutieusement une action pour contrer le risque d'une augmentation de la présence policière sur le lieu de l'action. Par exemple :

- Tu peux faire une **reconnaissance (#2)** rigoureuse du lieu de l'action et préparer un bon plan de fuite.
- Si tu prévois de commettre un incendie volontaire, tu peux utiliser un engin incendiaire avec un retardateur pour que l'engin ne s'active qu'après ton départ du lieu de l'action.
- Tu peux profiter du fait qu'une augmentation de la présence policière à un endroit peut signifier une diminution de la présence policière à un autre endroit.

4.2. Cartographie de réseau

Utilisée par les tactiques : **Incrimination (p. 15)**

La cartographie de réseau est le processus par lequel un adversaire apprend à connaître l'organisation et les relations sociales d'un réseau donné. En acquérant cette connaissance, un adversaire peut sélectionner des individus à surveiller de plus près, à arrêter, ou à recruter comme **indics (p. 26)**.

L'État utilise très fréquemment les listes d'amis sur les réseaux sociaux (une forme d'**open-source intelligence (p. 28)**) pour la cartographie de réseau car cela ne demande pas de mandat ou d'autorisation légale.

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques, et en particulier utiliser des applications de messagerie chiffrées de bout-en-bout sur des appareils chiffrés, pour dissimuler tes ré-

[10] https://crimethinc.com/2017/08/07/total-policing-total-defiance-the-2017-g20-and-the-battle-of-hamburg-a-full-account-and-analysis

seaux sociaux et faire que ce soit plus difficile pour un adversaire de cartographier ton réseau.

Cloisonnement (#2) : Tu peux cloisonner tes différentes activités (ou projets) pour que ce soit plus difficile pour un adversaire de cartographier ton réseau.

Dessiner une carte de son réseau (#2) : Un adversaire peut cartographier un réseau en utilisant des infiltré·e·s et des indics pour surveiller le réseau : les infiltré·e·s et indics se font connaître en se liant petit à petit aux gens, identifient les profils sociaux des personnes du réseau, trouvent des points de pression pour instiguer des conflits interpersonnels et politiques, et piègent les gens. Pour contrer ça, tu peux dessiner une carte de ton réseau pour rendre ton réseau plus résilient face aux tentatives d'infiltration et t'assurer qu'il ne place pas sa confiance dans des personnes qui pourraient être ou devenir des indics.

Fausse identité (#2) : Pendant une vérification d'identité, tu peux présenter une fausse identité pour que ce soit plus difficile pour l'État de cartographier ton réseau.

Principe du *need-to-know* (#2) : Tu peux appliquer le principe du *need-to-know* pour que ce soit plus difficile pour un adversaire de cartographier ton réseau.

Téléphones anonymes (#2) : Tu peux utiliser des téléphones anonymes pour que ce soit plus difficile pour un adversaire de cartographier ton réseau.

Éviter l'auto-incrimination (#2) : Un adversaire peut utiliser des informations obtenues par de l'auto-incrimination pour mettre en danger non seulement la personne dont les informations proviennent, mais aussi le reste de son réseau. Pour contrer ça, tu ne devrais en aucun cas parler à un adversaire, et tu devrais éviter de fournir tes informations biométriques (photo du visage, empreintes digitales, ADN) si possible.

Opérations répressives

Mauvaises intentions (#2) : Pour prouver que les accusé·e·s se connaissaient et étaient donc probablement complices, les enquêteurs ont utilisé plusieurs indices[11] :

- Iels avaient été arrêté·e·s aux mêmes manifestations.
- Iels s'appelaient au téléphone régulièrement.
- Iels avaient vécu aux mêmes endroits pendant de longues périodes, comme le montraient leurs relevés téléphoniques.

4.3. Chiens de détection

Utilisée par les tactiques : **Arrestation (p. 15)**, **Incrimination (p. 15)**

Les chiens de détection sont des chiens qui ont été entraînés par un adversaire pour détecter certaines substances, principalement grâce à leur odorat.

Un adversaire peut amener des chiens de détection sur le lieu d'une action peu après l'action et leur faire suivre une odeur. Si les chiens détectent et suivent ton odeur avec succès, cela pourrait donner des indices à l'adversaire sur l'itinéraire que tu as suivi pour quitter le lieu de l'action, voir le mener à toi. Il est plus facile pour des chiens de détection de suivre une odeur en zone rurale qu'en zone urbaine où la population est plus dense.

Mesures d'atténuation

Préparation minutieuse de l'action (#2) : Si tu penses que des chiens de détection peuvent être déployés après une action, tu peux prévoir de prendre des mesures appropriées en quittant le lieu de l'action. Par exemple, tu peux prévoir de traverser des étendues d'eau pour casser la piste que les chiens suivent, ou prévoir d'utiliser du spray au poivre sur la piste pour perturber l'odorat des chiens.

Opérations répressives

Fenix (#2) : Dans l'une des perquisitions, la police a utilisé des chiens de détection entraînés à détecter des explosifs[12].

Affaire de l'association de malfaiteurs de Bure (#2) : Des chiens de détection ont été utilisés dans l'une des perquisitions[13].

4.4. Collaboration des fournisseurs de service

Utilisée par les tactiques : **Incrimination (p. 15)**

[11] https://infokiosques.net/spip.php?article597

[12] https://antifenix.noblogs.org/post/2015/06/03/interview-with-an-activist-detained-during-operation-fenix

[13] Source non publique.

Éviter l'auto-incrimination (#2) : Un adversaire peut utiliser la science forensique appliquée au numérique pour extraire des informations auto-incriminantes d'un appareil numérique. Pour contrer ça, tu peux éviter de stocker de telles informations sur des appareils numériques à part pour des raisons mûrement réfléchies (par exemple écrire et envoyer un communiqué de revendication tout en adoptant de **bonnes pratiques numériques (#2)**).

Opérations répressives

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont analysé des supports de stockage en extrayant automatiquement les fichiers contenant les mots clés suivants en rapport avec l'enquête[13] :

- « Action ».
- « Andra », l'agence en charge du projet Cigéo.
- « Bindeuil », le nom du bâtiment attaqué pendant la manifestation du 21 juin 2017.
- « Hibou », un nom utilisé par des personnes en lutte contre Cigéo pour s'auto-désigner.
- « Incendie ».

4.17.9. Reconnaissance de démarche

La reconnaissance de démarche est l'analyse du style et du rythme de marche des individus, dans le but d'associer un style et rythme de marche à un autre.

La reconnaissance de démarche implique qu'un humain ou un système automatisé localise et mesure les caractéristiques corporelles (par exemple la position des chevilles, des genoux et des hanches) d'une personne en mouvement, et les compare avec les caractéristiques corporelles d'une autre personne. Si les caractéristiques corporelles sont suffisamment proches, on considère que les corps appartiennent à la même personne.

Les systèmes modernes de reconnaissance de démarche sont capables d'identifier une personne de très loin, même si elle essaie de modifier intentionnellement sa démarche.

Mesures d'atténuation

Dissimulation biométrique (#2) : Tu peux porter des vêtements amples qui cachent la forme de ton corps, utiliser un parapluie ou d'autres objets couvrants, ou changer drastiquement ton style de marche en adoptant une « démarche bizarre ».

Tenue anonyme (#2) : Tu peux porter des vêtements amples pour cacher ta démarche.

Opérations répressives

Bialystok (#2) : La principale preuve contre la personne accusée d'une attaque explosive contre un commissariat était une comparaison de sa démarche et de la couleur de son manteau avec les caractéristiques correspondantes d'une personne filmée par les caméras de surveillance du commissariat[69].

Scintilla (#2) : Deux des personnes ont été accusées d'avoir commis un incendie volontaire parce que leurs démarches et la forme de leurs corps ont été considérés compatibles avec des personnes filmées par des caméras de vidéosurveillance en train de placer un bidon de liquide inflammable devant un bureau de poste italien[70].

4.17.10. Reconnaissance faciale

La reconnaissance faciale est l'analyse des caractéristiques des visages humains dans le but d'associer un visage à un autre.

La reconnaissance faciale implique qu'un humain ou un système automatisé localise et mesure les caractéristiques (par exemple la forme du nez, la distance entre les yeux) d'un visage (ou d'une photo d'un visage), et les compare avec les caractéristiques d'un autre visage (ou photo d'un visage). Si les caractéristiques des deux visages sont suffisamment proches, on considère que les visages appartiennent à la même personne.

Les systèmes modernes de reconnaissance faciale sont capables de comparer la photo d'un visage à une vaste base de données de visages, même si le visage est masqué, avec seulement les yeux et sourcils visibles. Des systèmes de reconnaissance faciale associés à la **vidéosurveillance de masse (p. 41)** peuvent être utilisés pour automatiser le suivi d'individus à travers un espace.

Voir le sujet « Reconnaissance faciale »[71].

[69] https://ilrovescio.info/2022/02/02/aggiornamento-sulle-misure-e-sul-processo-per-lop-byalistok

[70] https://macerie.org/index.php/2019/04/17/ultime-da-carceri-e-tribunali

[71] https://notrace.how/resources/fr/#topic=facial-recognition

L'identification de la voix peut être utilisée pour déterminer, par exemple :

- Qui parle sur une conversation téléphonique interceptée ou un enregistrement fait par un **microphone caché (p. 22)**.
- Qui a appelé les autorités pour faire une alerte à la bombe.

Voir aussi

À propos d'identification de l'auteur :

- Counteracting Forensic Linguistics[67] (*Contrer la science forensique appliquée à la linguistique*).
- Qui a écrit ça?[68].

Mesures d'atténuation

Dissimulation biométrique (#2) : Tu peux cacher les propriétés accoustiques de ta voix pour contrer l'identification de la voix.

Masquer son style d'écriture (#2) : Tu peux cacher ton style d'écriture pour contrer l'identification de l'auteur.

Opérations répressives

Scripta Manent (#2) : Des textes publiés par certain·e·s des accusé·e·s ont été comparés aux communiqués de revendication de la Fédération Anarchiste Informelle, dans le but de prouver que les accusé·e·s avaient écrit ces communiqués[62].

4.17.8. Numérique

Un Cellebrite Universal Forensics Extraction Device (UFED) qui extrait les données d'un iPhone 4S, 2013.

[67] https://anonymousplanet.org/guide.html#appendix-a4-counteracting-forensic-linguistics

[68] https://notrace.how/resources/fr/#qui-a-ecrit

La science forensique appliquée au numérique est l'extraction, le stockage, et l'analyse des données numériques qui peuvent être utiles dans le cadre d'enquêtes. Cela inclut les données provenant d'ordinateurs, de téléphones, de disques dur, et autres supports de stockage.

Par exemple, cette discipline peut être utilisée pour récupérer un fichier « supprimé » du disque dur d'un ordinateur, récupérer l'historique de navigation web d'un téléphone, ou déterminer comment un serveur a été piraté.

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Un adversaire peut utiliser la science forensique appliquée au numérique pour extraire des données d'un appareil numérique que tu as utilisé. Pour contrer ça, tu peux adopter de bonnes pratiques numériques et, en particulier, utiliser Tails[9], un système d'exploitation « amnésique » conçu pour ne pas laisser de traces sur l'ordinateur sur lequel il est utilisé.

Lorsqu'il enquête sur une cyber-action, un adversaire peut utiliser la science forensique appliquée au numérique pour analyser les cibles de l'action et déterminer d'où provient l'action, un processus appelé *attribution* qui peut impliquer de déteminer quels outils ont été utilisés pour l'action et toute autre « signature » numérique. Quand tu effectues une cyber-action, tu peux adopter de bonnes pratiques numériques pour que ce soit plus difficile pour un adversaire de réussir cette attribution. Par exemple, tu peux :

- Utiliser des outils populaires plutôt que sur mesure.
- Si tu utilises un Virtual Private Server (VPS), **achète-le anonymement (#2)** et accède-y avec Tails[9].

Chiffrement (#2) : Un adversaire peut utiliser la science forensique appliquée au numérique pour extraire des données d'appareils numériques non chiffrés. Pour contrer ça, tu peux chiffrer tes appareils numériques avec le chiffrement complet du disque et un mot de passe robuste.

Effacement et protection des métadonnées (#2) : Un adversaire peut utiliser la science forensique appliquée au numérique pour extraire et analyser des métadonnées. Pour contrer ça, tu peux effacer les métadonnées de fichiers avant de les publier en ligne ou de les envoyer à des gens.

La collaboration des fournisseurs de service est le processus par lequel une entité qui a des informations à propos de toi parce qu'elle te fournit un service fournit ces informations à un adversaire. La collaboration des fournisseurs de service peut fournir aussi bien des informations actuelles qu'historiques.

L'État peut légalement contraindre les fournisseurs de service à fournir des informations, en fonction du contexte. Par exemple :

- L'Espagne, un État avec un haut degré de contrôle sur les entreprises situées sous sa juridiction, peut très facilement contraindre les opérateurs de téléphonie mobile espagnols à fournir des informations sur les usagers espagnols du réseau de téléphonie mobile.
- l'Iran, un État sans relations diplomatiques avec le Canada, ne peut pas contraindre l'Agence du revenu du Canada à fournir des informations sur les contribuables canadiens.

Des adversaires non-étatiques comme étatiques peuvent obtenir les informations de fournisseurs de service par :

- La corruption : acheter les informations de fournisseurs de service vendues par des individus corrompus ayant accès aux informations (par exemple des employés du fournisseur de service, des policiers).
- Des fuites de données[14] : obtenir les informations de fournisseurs de service via la révélation, divulgation, ou perte non-autorisées des informations (par exemple, la base de données d'un fournisseur de service est piratée et un adversaire l'achète sur le marché noir).

4.4.1. Autres

Les fournisseurs de service autres que les opérateurs de téléphonie mobile peuvent fournir des informations à propos de toi à un adversaire.

Institutions d\'État

Les institutions d'État peuvent fournir toute information qu'ils ont à propos de toi, y compris ton adresse, tes relevés d'impôts, ton dossier médical, etc.

[14] https://fr.wikipedia.org/wiki/Fuite_d'information

Magasins

Les magasins physiques et en ligne peuvent fournir des informations à propos d'achats faits via le magasin, y compris :

- À partir d'un nom : les objets achetés sous ce nom, ainsi que la date des achats.
- À partir d'un objet ou d'une catégorie d'objets : les noms des personnes qui ont acheté l'objet, ainsi que la date des achats.

De plus, les magasins physiques peuvent fournir :

- Les images de vidéosurveillance des caméras du magasin.
- Les témoignages d'employé·e·s du magasin, par exemple à propos de l'apparence physique d'une personne qui a fait un achat particulier.

Banques

Les banques peuvent fournir :

- L'activité de ton compte bancaire, y compris la date, l'emplacement, et le montant de tout achat ou retrait fait avec une carte.
- Les images de vidéosurveillance des caméras sur les Distributeurs Automatiques de Billets (DAB).

Fournisseurs d\'accès à Internet

Les fournisseurs d'accès à Internet peuvent fournir :

- Si tu adoptes de **bonnes pratiques numériques (#2)** et que tu utilises Tor : les métadonnées à propos de tes activités Internet, comme par exemple quand est-ce que tu utilises Internet.
- Si tu n'utilises pas Tor : tes activités Internet, y compris la liste des sites web que tu visites.

Services en ligne

Les sites web, fournisseurs d'email, et autres services en ligne peuvent fournir :

- Le contenu des communications non chiffrées que tu as sur le service (par exemple les publications sur les réseaux sociaux, les mails non chiffrés).
- Les métadonnées des communications chiffrées que tu as sur le service (par exemple l'expéditeur, le destinataire, et la date des emails chiffrés).

Mesures d'atténuation

Achats anonymes (#2) : Si tu dois acheter un objet dans un magasin, tu peux l'acheter anonymement pour que ce soit plus difficile pour un adversaire d'utiliser la collaboration du magasin pour relier ton identité à l'objet.

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques pour que ce soit plus difficile pour des fournisseurs de service de fournir des informations utiles à un adversaire. Par exemple, tu peux :

- Utiliser Tor[15] pour que ce soit plus difficile pour ton fournisseur d'accès à Internet de fournir des informations utiles à propos de tes activités Internet à un adversaire.
- Utiliser des services en ligne de confiance[16] qui refuseront d'obtempérer aux requêtes d'un adversaire d'accéder à tes données, ou construiront leur service pour que ce soit techniquement impossible d'obtempérer à de telles requêtes.

Chiffrement (#2) : Tu peux chiffrer les données « en mouvement » pour que ce soit plus difficile pour des fournisseurs de service de fournir des informations utiles à un adversaire.

Opérations répressives

Répression contre Zündlumpen (#2) : Un indice contre une éditrice présumée du journal était qu'elle a utilisé son compte bancaire pour commander des choses qui pourraient être utilisées dans une imprimerie—ses relevés bancaires ont vraisemblablement été obtenus par les enquêteurs avec la collaboration de la banque[17].

Répression du sabotage de l'usine Lafarge (#2) : Les enquêteurs ont donné le numéro de série d'un appareil photo au fabricant de l'appareil, et le fabricant leur a donné le nom du magasin où l'appareil avait été vendu[18]. Cela a aidé les enquêteurs à identifier une personne qu'ils ont accusé d'avoir pris des photos avec l'appareil.

Opération contre Peppy et Krystal (#2) : Un magasin de feux d'artifice a fourni aux enquêteurs des fichiers montrant que Peppy avait acheté des feux d'artifice au magasin trois jours avant la manifestation[19].

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont utilisé la collaboration de banques pour obtenir les relevés bancaires d'associations luttant contre Cigéo[13]. Les relevés bancaires d'une association comportaient un transfert de 500€ intitulé « participation manif 18 fev », en référence à une manifestation lors de laquelle des personnes ont attaqué un bâtiment en lien avec Cigéo.

Le propriétaire d'un supermarché dans une ville à environ 20 km de Bure a prévenu les enquêteurs qu'il avait vu des clients acheter une quantité inhabituelle d'alcool à brûler (15 litres), et a donné le ticket de caisse aux enquêteurs.

4.4.2. Opérateurs de téléphonie mobile

Les opérateurs de téléphonie mobile peuvent fournir des informations à propos de toi à un adversaire.

Ils peuvent fournir :

- À partir d'un nom : les numéros de téléphone enregistrés sous ce nom.
- À partir d'un numéro de téléphone : le nom sous lequel le numéro de téléphone est enregistré et le numéro IMEI[20] du téléphone dans lequel le numéro de téléphone est utilisé.
- À partir d'un numéro IMEI : le numéro de téléphone qui est utilisé dans le téléphone avec ce numéro IMEI.

De plus, à partir de ton numéro de téléphone, les opérateurs de téléphonie mobile peuvent fournir des données et métadonnées (actuelles et historiques) relatives à ton activité téléphonique :

- Le contenu des SMS et des appels classiques que tu fais sur ton téléphone.
- La liste des sites web que tu visites sur ton téléphone.
- La position physique de ton téléphone.

[15] https://torproject.org/fr
[16] https://riseup.net/en/security/resources/radical-servers
[17] https://notrace.how/resources/fr/#chretien-de-baviere
[18] https://notrace.how/resources/fr/#lafarge
[19] https://notrace.how/documentation/case-against-peppy-and-krystal-affidavit.pdf
[20] Un numéro International Mobile Equipment Identity (IMEI, identité internationale d'équipement mobile) est un numéro qui identifie un téléphone de manière unique.

Gants (#2) : Tu peux porter des gants pour éviter de laisser des empreintes digitales sur les surfaces que tu touches.

Préparation minutieuse de l'action (#2) : Un adversaire peut utiliser la science forensique appliquée aux empreintes digitales pour collecter et analyser des empreintes digitales sur le lieu d'une action. Pour contrer ça, tu peux préparer minutieusement l'action pour que tous les outils que tu prévoies d'utiliser pendant l'action soient dépourvus d'empreintes digitales au cas où tu les perdes ou tu aies besoin de t'en débarrasser dans un endroit où ils pourraient être récupérés par un adversaire.

Opérations répressives

Affaire de l'association de malfaiteurs de Bure (#2) : Des empreintes digitales ont été prélevées sur des objets trouvés dans des perquisitions, dont un carnet, des feuilles de papier, des masques à gaz, des cocktails Molotov, et des récipients contenant de l'essence ou autres substances. La grande majorité des empreintes digitales prélevées n'ont correspondu à personne. Certaines des empreintes digitales prélevées ont correspondu à des individus dans le Fichier automatisé des empreintes digitales (FAED)[13].

4.17.6. Incendie volontaire

La science forensique appliquée aux incendies volontaires (aussi connue sous le nom d'*investigations incendie*) est l'application de la science aux enquêtes sur des incendies volontaires. Cette discipline comporte deux phases distinctes : l'analyse de la scène de l'incendie, qui se concentre sur des preuves sur la scène elle-même, et l'analyse des résidus de l'incendie, qui se concentre sur des preuves retirées de la scène de l'incendie et analysées en laboratoire.

L'analyse de la scène de l'incendie consiste à déterminer si un feu est d'origine volontaire et à identifier son point de départ. Cette analyse est souvent beaucoup plus difficile si le point d'« embrasement » a été atteint—quand une pièce devient si chaude que toute surface inflammable prend feu.

L'analyse des résidus de l'incendie se concentre sur les résidus liquides inflammables et vise à identifier de potentielles traces d'accélérants et leurs compositions chimiques—ces échantillons sont souvent trouvés par des **chiens (p. 17)** sur la scène.

Mesures d'atténuation

Achats anonymes (#2) : Un adversaire peut parfois identifier des accélérants et les relier à une marque de station-service, et à partir de là à l'identité de la personne qui a acheté les accélérants. Pour contrer ça, tu peux acheter des accélérants anonymement.

Préparation minutieuse de l'action (#2) : Un adversaire peut relier plusieurs actions ensemble si des accélérants de la même source ont été utilisés dans toutes les actions. Pour contrer ça, tu peux éviter de réutiliser des accélérants d'une même source dans des actions différentes.

Opérations répressives

Affaire de l'association de malfaiteurs de Bure (#2) : Des traces d'accélérants ont été collectées sur des objets récupérés après des manifestations, et analysées[13].

4.17.7. Linguistique

La science forensique appliquée à la linguistique est l'application de connaissances linguistiques pour identifier l'auteur d'un texte ou la personne derrière une voix. L'identification de l'auteur (aussi appelée *stylométrie*) est basée sur l'analyse de certains schémas d'utilisation du langage : vocabulaire, collocations, orthographe, grammaire, etc. L'identification de la voix est basée sur les unités phonétiques et les caractéristiques accoustiques de la voix.

Identification de l\'auteur

L'identification de l'auteur peut être utilisée pour déterminer, par exemple :

- Qui a écrit un communiqué de revendication anonyme publié sur Internet ou envoyé à un journal.
- Si plusieurs communiqués de revendication anonymes ont été écrits par la même personne ou le même groupe.
- Qui a rédigé un plan relatif à des activités illégales trouvé pendant une **perquisition (p. 30)**, une **visite discrète de domicile (p. 53)** ou une arrestation.

Identification de la voix

pante correspondant aux coupures faites dans la clôture du lieu de la tentative d'incendie de mai[51].

Affaire du 8 décembre (#2) : Pendant les perquisitions, plusieurs objets (gazinière, poêles, gants, spatules) ont été analysés pour y chercher des traces de produits pouvant servir à fabriquer des explosifs[37].

4.17.4. Balistique

Sur la gauche, une balle 9mm qui n'a pas été utilisée. Sur la droite, une balle du même modèle qui a été utilisée.

La science forensique appliquée à la balistique (aussi connue sous le nom de *balistique judiciaire*) est l'application de la science aux enquêtes sur les armes à feu et les balles. Quand une balle est tirée depuis une arme à feu, l'arme laisse des marques microscopiques sur la balle et sa douille. Ces marques sont des sortes d'empreintes digitales balistiques.

Quand un adversaire récupère une balle, des experts balistiques peuvent tirer avec l'arme à feu d'un suspect puis comparer les marques sur la balle récupérée aux marques sur la balle qu'ils ont tiré. Les douilles sont comparées de la même façon.

Mesures d'atténuation

Achats anonymes (#2) : Un adversaire peut utiliser la science forensique appliquée à la balistique pour relier une arme à feu ou une balle à un vendeur, et de là à l'identité de la personne qui a acheté l'arme ou la balle. Pour contrer ça, tu peux acheter des armes à feu et des balles anonymement, par exemple grâce à des connexions à des réseaux de crime organisé ou à la fraude.

Cachette ou planque (#2) : Un adversaire a besoin d'avoir accès à une arme à feu pour faire une analyse balistique de l'arme. Pour contrer ça, tu peux stocker l'arme à feu dans une cachette ou une planque.

4.17.5. Empreintes digitales

Les plis sur un doigt humain.

La science forensique appliquée aux empreintes digitales est la collecte, le stockage et l'analyse des traces laissées par les plis présents sur les doigts humains.

Des empreintes digitales sont laissées sur les surfaces que tu touches par l'humidité et la graisse sur tes doigts, et peuvent être prélevées sur ces surfaces. Elles peuvent aussi être prélevées directement depuis tes doigts avec de l'encre ou d'autres substances (les doigts sont d'abord trempés dans l'encre, puis posés sur du papier, laissant des empreintes sur le papier), ou avec des scanners d'empreintes électroniques.

Parce que les empreintes digitales sont presque uniques et sont stables au cours de la vie d'un individu, deux empreintes digitales peuvent être comparées pour déterminer si elles appartiennent au même individu.

Les empreintes digitales laissées sur des surfaces se dégradent avec le temps et sous certaines conditions (par exemple en contact avec de l'acétone), et doivent contenir une quantité suffisante de détails pour être utilisables pour une comparaison. Sur certaines surfaces, comme le métal, la réaction entre la graisse des doigts et le métal peut laisser une empreinte dans le surface elle-même, de telle sorte que l'empreinte digitale reste identifiable même après avoir nettoyé la surface avec un chiffon imbibé d'acétone.

Dans de nombreux pays, l'État a des bases de données d'empreintes digitales contenant les empreintes digitales de nombreux individus, souvent obtenues lors d'arrestations ou après des condamnations.

Voir le sujet « Empreintes digitales »[66].

Mesures d'atténuation

[66] https://notrace.how/resources/fr/#topic=fingerprints

- Des métadonnées à propos de ton utilisation d'applications de messagerie chiffrées de bout-en-bout (par exemple, quand est-ce que tu utilises Signal et la taille approximative des messages envoyés et reçus sur Signal).

Cela signifie que n'importe laquelle des conditions suivantes peut permettre à un adversaire, avec la collaboration des opérateurs de téléphonie mobile, d'accéder aux données et métadonnées (actuelles et historiques) relatives à ton activité téléphonique :

- Connaître ton nom (si ton téléphone n'est pas **anonyme (#2)**).
- Connaître ton numéro de téléphone, qu'il peut trouver en surveillant ou en saisissant le téléphone d'un de tes contacts, en utilisant un **IMSI-catcher (p. 45)**, ou grâce à des techniques de corrélation avancées[21].
- Connaître le numéro IMEI de ton téléphone, qu'il peut trouver en saisissant ton téléphone.

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques pour que ce soit plus difficile pour des opérateurs de téléphonie mobile de fournir des informations utiles à un adversaire. Par exemple, tu peux utiliser des applications de messagerie chiffrées de bout-en-bout sur ton téléphone, plutôt que des SMS et appels classiques.

Chiffrement (#2) : Tu peux chiffrer les données « en mouvement » pour que ce soit plus difficile pour des opérateurs de téléphonie mobile de fournir des informations utiles à un adversaire.

Téléphones anonymes (#2) : Tu peux utiliser des téléphones anonymes pour que ce soit plus difficile pour des opérateurs de téléphonie mobile de fournir des informations utiles à un adversaire.

Opérations répressives

Opération contre Boris (#2) : Les enquêteurs ont utilisé la collaboration d'opérateurs de téléphonie mobile pour intercepter des appels reçus ou émis depuis le téléphone de Boris et les téléphones de personnes proches de lui[22]. Ils ont fréquemment écouté en temps réel les appels interceptés et utilisé les informations ainsi obtenues pour ajuster des opérations de **surveillance physique (p. 47)** en cours.

Les enquêteurs ont utilisé la collaboration d'un fournisseur d'email pour accéder en temps réel à une adresse email utilisée par Boris : ils étaient capables de voir en temps réel les emails envoyés et reçus.

Mauvaises intentions (#2) : Les enquêteurs ont utilisé la collaboration des opérateurs de téléphonie mobile pour relier des numéros de téléphone à des identités civiles, pour savoir quels numéros de téléphone étaient en contact, pour géolocaliser des téléphones (rétrospectivement et en temps réel) et pour enregistrer des appels téléphoniques[11].

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont utilisé la collaboration des opérateurs de téléphonie mobile pour[13] :

- Faire des liens entre des gens.
- Géolocaliser des téléphones en temps réel.
- Enregistrer un grand nombre de conversations téléphoniques, dont des conversations ayant eu lieu entre le moment où un appel était passé et le moment où le destinataire décrochait (c'est-à-dire pendant que le téléphone sonnait).
- Identifier les numéros de téléphone qui avaient été actifs autour de Bure pendant trois manifestations ayant eu lieu en février, juin, et août 2017, dont 55 numéros de téléphones qui avaient été actifs pendant chacune de ces trois manifestations.

4.5. Construction parallèle

Utilisée par les tactiques : **Incrimination (p. 15)**

La construction parallèle est le processus illégal par lequel la police construit une chaîne de preuves parallèle, ou séparée, dans une enquête afin de cacher la manière dont l'enquête s'est réellement déroulée.

Par exemple, une agence de renseignements peut collecter des preuves numériques incriminantes depuis un téléphone sans mandat, puis faire une **perquisition (p. 30)** pour saisir le téléphone où ces preuves peuvent être « dé-

[21] Par exemple, si un adversaire sait que tu étais dans un endroit A lundi et un endroit B mardi, et sait grâce aux données des antennes téléphoniques qu'un certain téléphone était le seul téléphone qui était aussi dans l'endroit A lundi et l'endroit B mardi, il peut déduire que le téléphone t'appartient.

[22] https://rupture.noblogs.org/post/2023/10/04/no-bars

couvertes » de manière à ce qu'elles ne soient pas rejetées lors du procès pour avoir été obtenues illégalement.

Une forme particulière de construction parallèle est le blanchiment de preuves, dans lequel un policier collecte illégalement des preuves puis les « blanchit » en les passant à un second policier qui les développe puis les apporte aux procureurs.

4.6. Coopération internationale

Utilisée par les tactiques : **Arrestation (p. 15)**, **Incrimination (p. 15)**

La coopération internationale est l'échange d'informations entre les agences de maintien de l'ordre et de renseignement de différents pays.

La coopération internationale peut être utilisée pour :

- Échanger des renseignements.
- Faciliter l'incrimination, l'arrestation et l'expulsion de suspects au-delà des frontières nationales.

La coopération internationale peut se produire par des canaux informels, ou via des organisations formelles comme Interpol.

Opérations répressives

Bialystok (#2) : En juin 2020, des personnes ont été arrêtées en Espagne et en France, grâce à une coopération entre des agences de police et de renseignement italiennes, espagnoles et françaises[23].

Lors de l'enquête, les policiers italiens ont essayé de cibler une personne vivant en Allemagne[24]. Ils ont envoyé plusieurs requêtes à la police allemande pour que la personne soit extradée ou que son domicile soit perquisitionné mais les requêtes ont été rejetées.

Scintilla (#2) : Carla a été arrêtée en France grâce à une coopération entre des agences de police et de renseignement italiennes et françaises[25].

Affaire de l'association de malfaiteurs de Bure (#2) : Certaines des personnes arrêtées avaient participé à des manifestations contre le sommet du G20 à Hambourg, en Allemagne[13]. Pour cette raison, des enquêteurs allemands ont coopéré avec les enquêteurs français, notamment en étant présents lorsque les personnes ont été interrogées après leur arrestation.

4.7. Dispositifs de surveillance cachés

Utilisée par les tactiques : **Incrimination (p. 15)**

Les dispositifs de surveillance cachés sont des appareils électroniques dissimulés par un adversaire pour collecter des données : audio, vidéo, et données de localisation.

Où

Un adversaire peut cacher des dispositifs de surveillance dans des bâtiments, dans ou sur des véhicules, ou en extérieur. Voici des emplacements notables :

- Des microphones et des caméras cachés au domicile d'une cible.
- Des dispositifs de surveillance par localisation cachés dans ou sur le véhicule d'une cible.
- Des caméras cachées aux fenêtres d'un bâtiment proche du domicile d'une cible, de telle sorte que les caméras filment l'entrée du domicile.

Quand

Un adversaire peut cacher des dispositifs de surveillance pour de la surveillance sur le long terme (par exemple des semaines, des mois ou des années) ou de la surveillance à court terme d'évènements particuliers. Un dispositif de surveillance caché peut disparaître :

- La plupart du temps, quand il est récupéré par ceux qui l'ont installé.
- Dans certains cas, quand il est découvert accidentellement par un tiers.
- Rarement, quand il est découvert intentionnellement (via une **recherche de dispositifs de surveillance (#2)**) et enlevé par un tiers.

Alimentation électrique

Les dispositifs de surveillance cachés ont besoin d'une alimentation électrique, qui peut être soit une batterie

[23] https://malacoda.noblogs.org/anarchici-imprigionati

[24] https://attaque.noblogs.org/post/2022/02/20/italie-allemagne-de-rome-a-bialystok-en-passant-par-berlin

[25] https://attaque.noblogs.org/post/2020/08/06/saint-etienne-arrestation-de-carla-recherchee-dans-le-cadre-de-loperation-scintilla

uniquement des lettres majuscules et faire des lettres les plus génériques possibles.

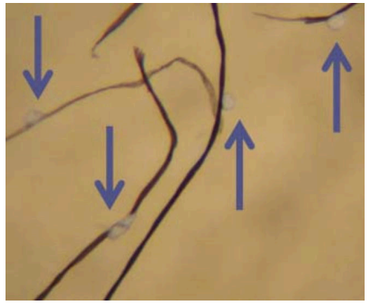
Opérations répressives

Scripta Manent (#2) : Des échantillons écrits de plusieurs des accusé·e·s (dont des notes saisies pendant des perquisitions et des lettres écrites depuis la prison) ont été comparés aux adresses écrites sur des colis piégés qui n'ont pas explosé, dans le but de relier les accusé·e·s aux attaques[62].

Opération de 2019-2020 contre Mónica et Francisco (#2) : Les étiquettes sur les deux colis piégés sont restées intactes—l'une parce que le colis n'a pas explosé, et l'autre malgré l'explosion du colis[46]. Les signatures manuscrites sur les étiquettes ont été comparées et correspondaient. Cela a montré que les colis avaient été envoyés par la même personne.

Répression du premier incendie de Jane's Revenge (#2) : Une comparaison entre le graffiti en écriture cursive laissé sur le lieu de l'action et des graffitis dans le même style faits quelques mois plus tard lors d'une manifestation ont aidé à identifier la personne[58].

4.17.3. Autres traces physiques



Goutelettes de peinture en spray adhérant aux fibres d'une veste, observées sous microscope (grossissement ~75x). En utilisant une bombe de peinture en spray, il est probable que des goutelettes de peinture issues de la vaporisation tombent sur les surfaces à proximité, et puissent être utilisées pour relier des vêtements à la peinture trouvée sur le lieu d'une action[63].

[62] https://lib.anarhija.net/library/operation-scripta-manent-in-italy-2016-2019#toc15

Les autres traces physiques sont les petits fragments de preuves physiques qui peuvent être transférés entre des objets, ou entre des objets et l'environnement. Ce transfert peut se produire quand deux objets se touchent, ou quand de petites particules se dispersent suite à une action ou mouvement. Ces traces physiques peuvent être analysées pour établir des liens entre des personnes, des objets, et des endroits.

Ces traces physiques incluent les poils (y compris les poils des animaux domestiques), les empreintes de pas, les résidus de tir, les fibres de vêtements, les particules de peintures, et les bouts de verre. Parmi les exemples moins courants, on trouve la terre, les cosmétiques, et les résidus d'incendie.

Voir le sujet « Autres traces physiques »[65].

Mesures d'atténuation

Cachette ou planque (#2) : Un adversaire peut utiliser des traces physiques pour relier des objets au lieu d'une action. Pour contrer ça, après l'action tu peux stocker dans une cachette ou une planque les outils qui sont trop chers pour que ce soit réaliste de s'en débarrasser après chaque action.

Préparation minutieuse de l'action (#2) : Un adversaire peut utiliser des traces physiques pour relier des objets au lieu d'une action. Pour contrer ça, tu peux minutieusement préparer l'action pour qu'après l'action tu te débarrasses de tous les outils et vêtements utilisés pendant l'action.

Tenue anonyme (#2) : Un adversaire peut utiliser des traces physiques issues de vêtements (par exemple des fibres textiles qui se détachent de vêtements dans l'environnement) pour établir des liens entre des personnes, des vêtements, et des endroits. Pour contrer ça, tu peux porter une tenue anonyme.

Opérations répressives

Opération contre Jeff Luers (#2) : Lors de la perquisition du garde-meubles, la police a trouvé une pince cou-

[63] *Handbook of Trace Evidence Analysis*[64] (2020), chapitre *Paints and Polymers*.

[64] http://sx3kelhcum7aaemtp27n2p3x4figvaymt2vibcabjpftxupzuu5ifzyd.onion/#handbook-of-trace-evidence-analysis

[65] https://notrace.how/resources/fr/#topic=other-physical-traces

des sous-vêtements en garde-à-vue, vraisemblablement pour y prélever son ADN[18].

Prometeo (#2) : Des traces ADN ont été utilisées pour condamner la personne accusée d'avoir brûlé un DAB[57].

Mauvaises intentions (#2) : Lors des gardes-à-vue, de l'ADN a été prélevé sur les vêtements des personnes et sur des gobelets en plastique[11]. Dans un cas, seulement neuf heures se sont écoulées entre le prélèvement d'une trace ADN en garde-à-vue et le résultat de sa comparaison à une autre trace prelevée antérieurement.

Les accusations contre une personne étaient basées sur une correspondance entre son ADN et l'ADN prelevé sur le lieu de la tentative d'incendie contre l'armoire électrique. Des traces ADN ont été prélevées sur un gant en latex trouvé à proximité et sur une bouteille à l'intérieur de l'armoire—qui n'a pas brûlé à cause d'un retardateur défectueux.

Les accusations contre d'autres personnes étaient basées sur une correspondance entre leur ADN et l'ADN prélevé sur une cigarette utilisée comme retardateur pour un engin incendiaire—le retardateur n'a pas fonctionné et a été retrouvé intact sous la dépanneuse de la police.

Répression du premier incendie de Jane's Revenge (#2) : En mai 2022, des traces ADN ont été prélevées sur plusieurs objets trouvés par les enquêteurs sur le lieu de l'action, dont une fenêtre cassée, un pot en verre, un briquet, et un cocktail Molotov intact[58]. En mars 2023, la police a vu la personne jeter un sac contenant un burrito en partie mangé dans une poubelle publique. Des traces ADN prélevées sur le contenu du sac correspondaient aux traces prélevées sur le lieu de l'action.

Scintilla (#2) : L'accusation contre Peppe était basée sur une correspondance entre des traces ADN trouvées à l'intérieur du colis piégé et son ADN prelevé sur un mégot de cigarette au cours de l'enquête[59].

Affaire de l'association de malfaiteurs de Bure (#2) : Des traces ADN ont été prélevées sur[13] :

- Des objets récupérés après des manifestations, dont des feux d'artifice, des cocktails Molotov, un briquet, et des cailloux utilisés pour briser des fenêtres.
- Des objets trouvés dans des perquisitions, dont des vêtements, des masques à gaz, des casques, et des récipients contenant de l'essence ou autres substances.

Les enquêteurs n'ont pas réussi à faire correspondre à qui que ce soit la grande majorité des traces ADN qu'ils ont prélevées. Les exceptions notables étaient :

- Une trace ADN sur un cocktail Molotov trouvé dans une perquisition a correspondu à une personne dans le Fichier national automatisé des empreintes génétiques (FNAEG).
- Une trace ADN sur le bouchon d'un bocal contenant des matières pouvant servir à construire des engins explosifs, trouvé dans une perquisition, a correspondu à une personne dans le FNAEG.
- Une trace ADN sur un briquet retrouvé après une manifestation a correspondu à une autre trace d'une affaire plus ancienne sans lien avec l'affaire en cours, mais n'a correspondu à personne dans le FNAEG.

Opération à Nea Filadelphia (#2) : Les accusations contre plusieurs personnes étaient basées sur une correspondance entre leur ADN, prélevé de force en garde-à-vue, et des traces ADN trouvées sur des « objets mobiles » près des lieux des braquages[60].

Panico (#2) : Des traces ADN étaient la seule preuve contre l'un·e des accusé·e·s[61].

4.17.2. Analyse de l'écriture

L'analyse de l'écriture est l'analyse d'échantillons écrits, typiquement dans le but d'associer un échantillon à un autre.

L'analyse de l'écriture est basée sur une compréhension des caractéristiques uniques de l'écriture de caractères et sur les processus physiologiques derrière l'écriture—les manières dont les facultés motrices d'une personne peuvent affecter son écriture.

Mesures d'atténuation

Dissimulation biométrique (#2) : Tu peux écrire sur des appareils numériques plutôt qu'à la main pour dissimuler ton écriture. En faisant un graffiti, tu peux utiliser

[57] https://roundrobin.info/2021/05/sentenza-beppe
[58] https://notrace.how/documentation/first-jane-s-revenge-arson-investigation-files.pdf
[59] https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto
[60] https://abcsolidaritycell.espivblogs.net/archives/130
[61] https://panicoanarchico.noblogs.org

soit le système électrique du bâtiment ou véhicule dans lequel le dispositif est caché, soit les deux. Dans de rares cas, il peut être alimenté par un câble Ethernet (*Power over Ethernet*, PoE). Pour économiser la batterie et que ce soit plus difficile de les détecter, les dispositifs peuvent ne pas être allumés en permanence.

Transmission de données

Les dispositifs de surveillance cachés transmettent souvent les données qu'ils collectent :

- Le plus souvent pour les dispositifs modernes bon marché, sur le réseau téléphonique à l'aide d'une carte SIM intégrée au dispositif.
- Dans certains cas via WiFi, Bluetooth, Ethernet, ou des fréquences radio arbitraires.

Certains dispositifs ne transmettent pas les données qu'ils collectent : pour récupérer les données, l'adversaire a besoin d'y accéder physiquement.

Voir aussi

- Ears and Eyes[26].
- Le sujet « Dispositifs cachés »[27].

4.7.1. Audio

Un microphone trouvé dans un néon à Modène, Italie, en décembre 2015[28].

Les dispositifs de surveillance cachés audio sont des appareils électroniques, typiquement des microphones, dissimulés par un adversaire pour collecter des données audio.

Un adversaire peut cacher des dispositifs de surveillance audio à tout endroit où des données audio intéressantes, typiquement des conversations, peuvent être collectées. Voici des emplacements notables :

- Le salon d'une cible.
- Le tableau de bord du véhicule d'une cible.
- Un endroit en extérieur où une cible rencontre régulièrement ou devrait bientôt rencontrer d'autres personnes.

Les dispositifs de surveillance cachés audio peuvent être très sensibles et enregistrer avec succès des conversations même quand il y a de la musique ou que les gens chuchotent. Ils peuvent être extrêmement petits—seulement quelques millimètres—surtout s'ils enregistrent localement (par exemple sur une carte SD) et ne transmettent pas leurs enregistrements.

Les conversations enregistrées peuvent être utilisées comme preuves lors d'un procès si des sujets incriminants sont discutés, ou si elles peuvent être déformées pour paraître incriminantes aux yeux d'un juge. Des conversations non-incriminantes et banales peuvent révéler beaucoup de choses sur des personnes surveillées et contribuer à la **cartographie de réseau (p. 16)**.

Voir Ears and Eyes[26] et le sujet « Dispositifs cachés »[27].

Mesures d'atténuation

Conversations en extérieur et sans appareils (#2) : Tu peux avoir des conversations sensibles en extérieur et sans appareils électroniques pour empêcher un adversaire d'enregistrer ces conversations avec des dispositifs de surveillance cachés audio.

Détection d'intrusion physique (#2) : Un adversaire doit souvent entrer discrètement dans un espace pour y installer un dispositif de surveillance caché audio. Tu peux prendre des mesures de détection d'intrusion physique pour détecter cette entrée discrète.

Recherche de dispositifs de surveillance (#2) : Tu peux rechercher des dispositifs de surveillance pour localiser des dispositifs de surveillance cachés audio et les retirer.

Opérations répressives

Renata (#2) : Six microphones cachés et une caméra ont été retrouvés dans une maison après l'opération[29]. Les microphones ont été retrouvés dans le salon, le couloir,

[26] https://notrace.how/earsandeyes/fr
[27] https://notrace.how/resources/fr/#topic=hidden-devices
[28] https://notrace.how/earsandeyes/fr/#modena-2015-12
[29] https://roundrobin.info/2019/03/trento-sei-microspie-e-una-telecamera-immagini-pesanti

et les chambres. La caméra a été retrouvée dans l'interphone.

Voir le cas Ears and Eyes[30] correspondant.

Scintilla (#2) : Des microphones cachés dans une maison pendant deux ans et demi ont enregistré des conversations que les enquêteurs ont utilisées pour prouver que les accusé·e·s se connaissaient, se parlaient régulièrement, s'inquiétaient de la création d'une base de données ADN nationale et de l'impossibilité de résister aux prélèvements ADN, et avaient discuté de l'écriture d'un texte qui devait être publié[31].

Voir le cas Ears and Eyes[32] correspondant.

4.7.2. Localisation

Une balise GPS retrouvée sous un véhicule à Berlin, en Allemagne, en août 2022[33].

Les dispositifs de surveillance cachés par localisation sont des appareils électroniques dissimulés par un adversaire pour collecter des données de localisation.

Un adversaire cache typiquement des dispositifs de surveillance par localisation dans ou sur le moyen de transport habituel d'une cible, comme une voiture ou un vélo.

Les dispositifs de surveillance cachés par localisation ont besoin d'un moyen de connaître leur propre position. Ils peuvent faire ça :

- Le plus souvent avec un GPS.
- Dans certains cas, avec des alternatives au GPS comme GLONASS ou des services de téléphonie par satellite.
- Plus rarement, en émettant des ondes radio réceptionnées par un opérateur de surveillance à proximité (typiquement dans un véhicule qui suit le véhicule de la cible).

Les données de localisation collectées peuvent être utilisées comme preuves lors d'un procès. Des données de localisations non-incriminantes et banales peuvent révéler beaucoup de choses sur des personnes surveillées et contribuer à la **cartographie de réseau (p. 16)**.

Voir Ears and Eyes[26] et le sujet « Dispositifs cachés »[27].

Mesures d'atténuation

Déplacement en vélo (#2) : Tu peux utiliser un vélo plutôt qu'un autre type de véhicule : contrairement aux autres véhicules, quand tu **recherches des dispositifs de surveillance (#2)** sur un vélo tu peux déterminer avec un haut degré de certitude si un dispositif de surveillance par localisation est installé sur le vélo ou non.

Tu devrais stocker le vélo en intérieur pour que ce soit plus difficile pour un adversaire d'installer un dispositif de surveillance par localisation dessus.

Détection d'intrusion physique (#2) : Un adversaire doit souvent entrer discrètement dans l'espace où un véhicule est garé pour cacher un dispositif de surveillance par localisation sur le véhicule. Tu peux prendre des mesures de détection d'intrusion physique pour détecter cette entrée discrète.

Recherche de dispositifs de surveillance (#2) : Tu peux rechercher des dispositifs de surveillance pour localiser des dispositifs de surveillance cachés par localisation et les retirer.

Opérations répressives

Opération contre Boris (#2) : Des balises GPS ont été installées sous plusieurs véhicules après que les enquêteurs aient appris que Boris—qui n'avait pas de permis de conduire—se faisait conduire dans ces véhicules[22].

Dans un cas, les enquêteurs ont appris à 14h30 via un appel téléphonique intercepté qu'une personne proche de Boris prévoyait d'emprunter un véhicule et de conduire Boris à une fête dans la soirée. Ils ont observé l'emprunt du véhicule, l'ont suivi jusqu'à la fête, ont attendu qu'il se gare, et à 21h45 ils avaient installé une balise dessus.

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont installé un dispositif de surveillance ca-

[30] https://notrace.how/earsandeyes/fr/#trento-2019-03
[31] https://macerie.org/index.php/2019/03/12/le-orecchie-della-pedrotta
[32] https://notrace.how/earsandeyes/fr/#torino-2019-03
[33] https://notrace.how/earsandeyes/fr/#berlin-2022-08

Bases de données ADN

Dans de nombreux pays, l'État a des bases de données ADN contenant les informations génétiques de nombreux individus, souvent obtenues lors d'arrestations ou après des condamnations.

Voir aussi

- « blablADN. Tout cramer pour brûler + longtemps : un guide pour ne pas laisser de traces[52] » pour une bonne vue d'ensemble de la science forensique appliquée à l'ADN.
- Le sujet « ADN »[53].

Mesures d'atténuation

Gants (#2) : Tu peux porter des gants pour éviter de laisser de l'ADN sur les surfaces que tu touches.

Protocoles de minimisation de l'ADN (#2) : Tu peux minimiser la quantité d'ADN que tu laisses sur une surface pour minimiser le risque qu'un adversaire puisse utiliser la science forensique appliquée à l'ADN pour aboutir à une conclusion utile à partir d'une analyse de la surface.

Préparation minutieuse de l'action (#2) : Un adversaire peut utiliser la science forensique appliquée à l'ADN pour prélever de l'ADN sur le lieu d'une action. Pour contrer ça, tu peux préparer minutieusement l'action pour minimiser les traces ADN sur le lieu de l'action. Par exemple, tu peux :

- Ranger tes cheveux sous un couvre-chef.
- Si tu dois découper une clôture, faire des trous suffisamment grands pour pouvoir passer à travers sans toucher la clôture.
- T'assurer que les surfaces sur le lieu de l'action ne soient pas touchées si ce n'est pas nécessaire, et que les surfaces avec lesquelles il faut interagir (comme une poignée de porte) soient touchées par une personne qui met en place des **protocoles de minimisation de l'ADN (#2)**.
- T'assurer que tout engin destructeur laissé sur place (par exemple un engin incendiaire avec retardateur) ait fonctionné comme prévu lors de tests réalisés dans des conditions similaires (température, etc.) L'objectif est de t'assurer que l'engin ne sera pas récupéré intact par un adversaire.
- T'assurer que rien n'est laissé sur place accidentellement comme un sac, un outil, ou quelque chose qui tombe d'une poche.

Opérations répressives

Scripta Manent (#2) : Des preuves ADN ont été utilisées pour condamner Alfredo Cospito[54].

Opération contre Boris (#2) : La seule preuve contre Boris était que son ADN a été trouvé sur un bouchon de bouteille au pied d'une des antennes brûlées dans le sabotage d'avril[22].

Lorsque l'ADN d'une personne proche de Boris a été prelevé pendant une perquisition, seulement huit heures et demi se sont écoulées entre le prélèvement de la trace ADN et le résultat de sa comparaison avec d'autres traces prélevées antérieurement.

Opération de 2019-2020 contre Mónica et Francisco (#2) : L'ADN de Francisco a été trouvé sur le colis piégé envoyé à l'ancien ministre de l'Intérieur, qui a été désamorcé et n'a pas explosé[46].

Répression contre Zündlumpen (#2) : Le seul indice contre un·e éditeur·ice présumé·e du journal était que son ADN a été trouvé sur un mégot de cigarette dans l'imprimerie perquisitionnée en avril 2022[17].

Renata (#2) : Après son arrestation et emprisonnement, la personne accusée de l'attaque explosive contre le siège social de Lega Nord à Trévise a refusé que son ADN soit prélevé[55]. Peu de temps après le refus de la personne, des matons ont cherché sa cellule et secrètement remplacé un peigne par un autre, vraisemblablement pour obtenir l'ADN de la personne à partir des cheveux sur le peigne qu'ils ont pris.

Répression du sabotage de l'usine Lafarge (#2) : Dans l'une des premières perquisitions, la police a insisté pour que les personnes arrêtées portent des masques chirurgicaux pour se protéger du Covid : les masques ont ensuite été saisis pour y prélever de l'ADN[56]. Une personne qui avait refusé de porter un masque s'est faite confisquer

[52] https://notrace.how/resources/fr/#blabladn
[53] https://notrace.how/resources/fr/#topic=dna
[54] https://insuscettibilediravvedimento.noblogs.org/post/2020/03/29/it-en-italia-su-una-sentenza-e-qualcosa-daltro-un-testo-di-marco-dal-carcere-di-alessandria
[55] https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha
[56] https://sansnom.noblogs.org/archives/16831

- Plusieurs supports de stockage non chiffrés qui contenaient des documents suspects.

Opération contre Jeff Luers (#2) : Lors de la perquisition du garde-meubles, les enquêteurs ont trouvé[51] :

- Des allume-feux correspondant à ceux trouvés sur le lieu de la tentative d'incendie de mai, ainsi que du matériel qui pouvait être utilisé pour fabriquer des engins incendiaires (bidons d'essence, éponges, bobines de fill et bâtonnets d'encens).
- Une pince coupante correspondant aux coupures faites dans la clôture du lieu de la tentative d'incendie de mai.

Affaire de l'association de malfaiteurs de Bure (#2) : Pendant les perquisitions, les enquêteurs ont trouvé[13] :

- Divers objets similaires à des objets utilisés dans des manifestations : récipients contenant de l'essence ou autres substances, feux d'artifice, cocktails Molotov, et un grand nombre de casques.
- Un sac à dos contenant à la fois un document écrit avec le nom d'une personne et des objets qui pourraient être utilisés pour construire des engins incendiaires ou explosifs.
- Un ordinateur non chiffré contenant à la fois le CV d'une personne et un document décrivant ce qui s'était passé pendant la manifestation du 21 juin 2017.
- De nombreux compte-rendus de réunions sensibles contenant les noms ou pseudos de personnes, à la fois sur papier et sur des supports de stockage non chiffrés.

Affaire du 8 décembre (#2) : Pendant les perquisitions, les enquêteurs ont trouvé des armes à feu et des produits pouvant servir à fabriquer des explosifs[37].

4.17. Science forensique

Utilisée par les tactiques : **Incrimination (p. 15)**

La science forensique est l'application de la science aux enquêtes pour la collecte, la préservation, et l'analyse de preuves. Elle recouvre un ensemble de domaines : analyse ADN, analyse d'empreintes digitales, analyse de tâches de sang, balistique judiciaire, analyse de traces laissées par des outils, sérologie, toxicologie, analyse de cheveux et de fibres, analyse d'empreintes de pas et de traces de pneus, analyse chimique des drogues, analyse de la peinture et des débris de verre, linguistique, analyse numérique du son, de la vidéo et de l'image, etc.

En plus de relier l'identité d'un suspect à une action, la science forensique est souvent utilisée pour relier ensemble des actions distinctes.

Les experts en science forensique témoignent souvent en tant qu'experts judiciaires lors de procès.

4.17.1. ADN

La science forensique appliquée à l'ADN (aussi connue sous le nom d'*analyses ADN*) est la collecte, le stockage, et l'analyse de traces ADN dans le but de faire correspondre des traces ADN à des individus.

Collecte

L'ADN est la molécule qui contient le code génétique des organismes. À l'exception des globules rouges, chaque cellule de ton corps contient de l'ADN. Tu fais tomber de l'ADN dans l'environnement en continu à travers les cellules de ta peau, tes poils, ta salive, ton sang, ta sueur, etc. Les traces ADN peuvent être prélevées depuis des corps humains ou depuis l'environnement et analysées dans des laboratoires spécialisés pour révéler des choses sur les individus dont elles proviennent.

Analyse

L'analyse d'une trace ADN peut fournir des informations basiques sur l'individu dont elle provient, comme son sexe génétique. La comparaison de deux traces ADN peut déterminer si elles appartiennent au même individu, à des individus proches génétiquement (par exemple des parents et leurs enfants, des cousin·e·s), ou à des individus éloignés génétiquement.

L'ADN dans l'environnement se dégrade au fil du temps et sous certaines conditions, et une trace ADN doit contenir une quantité suffisante d'ADN non-dégradé pour pouvoir être analysée avec succès. Avec les avancées technologiques, cette quantité diminue.

L'ADN est souvent traitée lors des procès comme une preuve infaillible qu'une personne a été en contact avec la surface sur laquelle son ADN a été trouvé.

[51] https://www.courtlistener.com/opinion/2627996/state-v-luers

ché par localisation sur un véhicule, qui est resté en place pendant environ un mois[13].

4.7.3. Vidéo

Une caméra trouvée derrière le vélux d'une école publique à Berlin, en Allemagne, en juillet 2011[34].

Les dispositifs de surveillance cachés vidéo sont des appareils électroniques, typiquement des caméras, dissimulés par un adversaire pour collecter des données vidéo.

Un adversaire peut cacher des dispositifs de surveillance vidéo à tout endroit d'où la cible ou zone sous surveillance est directement visible. Voici des emplacements notables :

- Le salon d'une cible.
- Les fenêtres d'un bâtiment proche du domicile d'une cible, avec une visibilité directe sur l'entrée du domicile.
- Près de **cachettes ou planques (#2)** comme cela s'est produit en Italie où des caméras à détection de mouvement ont été installées pour surveiller une cachette dans une forêt[35].

Les images enregistrées peuvent être utilisées comme preuves lors d'un procès. Des images non-incriminantes et banales peuvent révéler beaucoup de choses sur les personnes surveillées et contribuer à la **cartographie de réseau (p. 16)**.

Voir Ears and Eyes[26] et le sujet « Dispositifs cachés »[27].

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Un adversaire peut installer des dispositifs de surveillance cachés vidéo qui filment l'écran d'un ordinateur ou d'un téléphone, ou le clavier d'un ordinateur. Pour contrer ça, quand tu utilises un ordinateur ou un téléphone pour des activités sensibles, tu peux :

- Garder l'appareil orienté vers un mur que tu peux inspecter minutieusement pour y chercher des dispositifs de surveillance vidéo (plutôt qu'orienté vers une fenêtre ou une télévision, par exemple).
- Entrer tes mots de passe en te mettant sous un drap ou une couverture opaque.

Cachette ou planque (#2) : Tu peux garder du matériel d'action dans une cachette ou une planque pour éviter de le ramener chez toi, où des dispositifs de surveillance cachés vidéo peuvent être présents.

Détection d'intrusion physique (#2) : Un adversaire doit souvent entrer discrètement dans un espace pour y installer un dispositif de surveillance caché vidéo. Tu peux prendre des mesures de détection d'intrusion physique pour détecter cette entrée discrète.

Détection de surveillance (#2) : Un adversaire peut garer un véhicule de surveillance près de ton domicile avec une caméra qui filme l'entrée du domicile. Pour contrer ça, tu peux uiliser la technique suivante de détection passive de surveillance. Cela fonctionne uniquement si tu vis dans un endroit où il n'y a pas trop de véhicules différents qui se garent, c'est-à-dire dans certaines zones urbaines résidentielles et dans la plupart des zones rurales. Chaque fois que tu quittes et retournes à ton domicile, tu prends note de tous les véhicules garés dans la rue qui ont une visibilité directe sur ton domicile. En essayant de ne pas avoir l'air trop suspect·e, tu notes leurs modèles, couleurs, et plaques d'immatriculation, soit en mémorisant les informations soit en les mettant par écrit. Après un certain temps passé à faire ça, tu connaîtras la « référence » des véhicules qui se garent dans ta rue, qui seront les véhicules des personnes qui habitent à proximité ou de leurs invités. Une fois que tu connais cette référence, tu pourras repérer les véhicules qui ne font pas partie de cette référence et les examiner discrètement pour voir si ce sont des véhicules de surveillance.

Recherche de dispositifs de surveillance (#2) : Tu peux rechercher des dispositifs de surveillance pour localiser des dispositifs de surveillance cachés vidéo et les retirer.

[34] https://notrace.how/earsandeyes/fr/#berlin-2011-07

[35] https://attaque.noblogs.org/post/2022/05/22/italie-vous-nous-trouverez-a-notre-place-car-nous-ne-saurions-rester-a-la-votre

Opérations répressives

Opération contre Boris (#2) : Des caméras ont été installées dans les rues près du domicile de Boris et près du domicile d'une personne proche de lui pour filmer les entrées des domiciles[22].

4.8. Doxing

Utilisée par les tactiques : **Dissuasion (p. 15)**

Le doxing est la pratique qui consiste à publier les informations personnelles d'une cible sans son consentement dans le but de lui nuire ou d'encourager d'autres à lui nuire. Elle est le plus souvent employée par des adversaires non-étatiques.

Le doxing utilise souvent des informations obtenues par l'**open-source intelligence (p. 28)**.

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques pour que ce soit plus difficile pour un adversaire de te *doxer*.

4.9. Fabrication de preuves

Utilisée par les tactiques : **Incrimination (p. 15)**

La fabrication de preuves est la création de fausses preuves, ou la falsification de vraies preuves, pour incriminer une cible.

Voici des exemples notables de fabrication de preuves :

- Mentir dans un rapport de police.
- Placer du matériel incriminant pour faire accuser quelqu'un. Par exemple, des policiers à Baltimore (États-Unis) ignoraient que leurs caméras-piéton continuaient d'enregistrer après avoir été éteintes et se sont filmés en train de placer des drogues dans le sac d'un suspect.

En fonction du contexte, la fabrication de preuves peut être courante ou rare.

Mesures d'atténuation

Détection d'intrusion physique (#2) : Un adversaire doit souvent entrer discrètement dans un espace pour y placer des preuves fabriquées. Tu peux prendre des mesures de détection d'intrusion physique pour détecter cette entrée discrète.

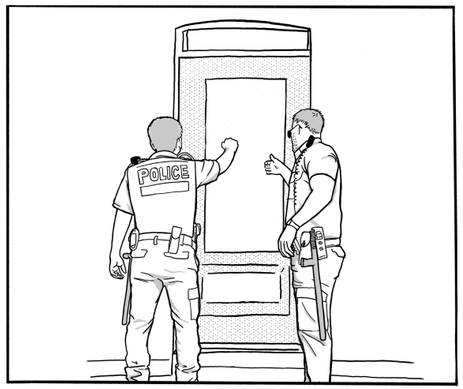
Opérations répressives

Prometeo (#2) : Les enquêteurs ont déformé des conversations obtenues grâce à des interceptions téléphoniques pour les rendre suspectes[36]. Par exemple, pendant une conversation téléphonique impliquant l'un·e des accusé·e·s, la phrase « tutta questa tensione sociale prima o poi scoppierà » (« toute cette tension sociale va, tôt ou tard, exploser ») a été prononcée, et a été seulement partiellement retranscrite dans les fichiers de l'enquête, devenant « prima o poi scoppierà » (« va, tôt ou tard, exploser »).

Affaire du 8 décembre (#2) : Les enquêteurs ont mal retranscrit ou déformé certaines conversations obtenues par des interceptions téléphoniques ou des dispositifs de surveillance cachés audio pour les rendre suspectes. Par exemple, le terme « lunettes balistiques » utilisé dans une conversation a été retranscrit en « gilets balistiques » par les services de renseignements, et est devenu « gilets explosifs » dans un rapport des procureurs en charge de l'affaire[37].

4.10. Frapper aux portes

Utilisée par les tactiques : **Dissuasion (p. 15)**, **Incrimination (p. 15)**



[36] https://ilrovescio.info/2020/08/23/uno-scritto-di-natascia-dal-carcere-di-piacenza

[37] https://soutien812.blackblogs.org/wp-content/uploads/sites/1922/2023/11/CompteRenduProces_A4.pdf

4.16. Perquisition

Utilisée par les tactiques : **Arrestation (p. 15)**, **Incrimination (p. 15)**

Une perquisition c'est quand un adversaire fait une visite surprise d'un domicile pour saisir des objets, arrêter les occupant·e·s du domicile, ou installer des dispositifs de surveillance cachés.

Quand

Un adversaire peut faire une perquisition :

- Le plus souvent, tôt le matin quand les occupant·e·s du domicile dorment et sont pris·e·s par surprise.
- Dans certains cas, pendant la journée. Cela peut être le cas si l'objectif de la perquisition est de saisir des appareils numériques lorsqu'ils sont allumés (et donc que leur **chiffrement (#2)** n'est pas efficace). Dans ce cas, l'adversaire peut décider de faire la perquisition pendant la journée parce qu'il est plus probable que les appareils numériques soient allumés quand leurs utilisateurs sont éveillés, c'est-à-dire pendant la journée.

Pourquoi

Un adversaire peut faire une perquisition pour :

- Saisir des objets pour trouver des preuves ou faire de la **cartographie de réseau (p. 16)**. Parmi les objets couramment saisis, on trouve les appareils électroniques, les documents écrits, le matériel qui pourrait être utilisé dans des actions, et les vêtements. Dans certains cas, l'adversaire saisit des objets coûteux (par exemple des ordinateurs, du matériel d'imprimerie) dans le but de perturber les capacités d'organisation de ses cibles.
- Arrêter les occupant·e·s du domicile.
- Installer des **dispositifs de surveillance cachés (p. 21)** dans le domicile.

Considérations supplémentaires

Dans certains pays, lorsqu'il fait une perquisition, l'État n'est autorisé qu'à fouiller les chambres des personnes nommées dans un mandat.

Mesures d'atténuation

Cachette ou planque (#2) : Tu peux garder du matériel d'action qui n'a pas de fonction « légitime » dans une cachette ou une planque, ou, au pire, le laisser transiter chez toi seulement pendant très peu de temps.

Clandestinité (#2) : Si tu entres en clandestinité, un adversaire ne peut pas savoir où tu vis, et ne peut donc pas perquisitionner ton domicile.

Se préparer aux perquisitions (#2) : Tu peux te préparer pour une perquisition en minimisant la présence d'objets qui pourraient être problématiques en cas de perquisition.

Se préparer à la répression (#2) : Tu peux te préparer à la répression pour minimiser l'impact des perquisitions.

Opérations répressives

Scripta Manent (#2) : Une personne a été arrêtée après que des batteries et un manuel d'électricien aient été trouvés à son domicile lors d'une perquisition[47].

Renata (#2) : Pendant une perquisition, les policiers ont essayé de se rendre au sous-sol sans réveiller les personnes dans la maison, puis se sont plaints en privé de n'avoir pas pu cacher ce qu'ils voulaient cacher[48].

Répression du sabotage de l'usine Lafarge (#2) : Parmi les premières perquisitions, l'une était particulèrement rigoureuse : les policiers ont cherché sous les matelas, derrière les housses de canapé et dans chaque tiroir de chaque meuble, inspecté chaque livre, carnet et vêtement ainsi que la vaisselle, et vidé des paquets de pâtes et des bocaux fermés[49].

Opération de 2013 contre Mónica et Francisco (#2) : Lors d'une perquisition du domicile de Mónica et Francisco, les enquêteurs ont trouvé[50] :

- Plusieurs vêtements et autres accessoires que Mónica et Francisco avaient utilisés pendant l'action et qui étaient visibles sur des images de vidéosurveillance publique.

[47] https://web.archive.org/web/20170928080735/http://www.informa-azione.info/italia_repressione_5_nuovi_arresti_e_una_trentina_di_perquisizioni_per_attacchi_federazione_anarchica_informale

[48] https://infernourbano.altervista.org/che-si-sappia-comunicato-dal-trentino

[49] https://sansnom.noblogs.org/archives/16978

[50] https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf

Opérations répressives

Opération de 2019-2020 contre Mónica et Francisco (#2) : Les photos utilisées pour identifier Mónica and Francisco sur les images de vidéosurveillance publique ont été trouvées sur les réseaux sociaux[46].

Répression du sabotage de l'usine Lafarge (#2) : Les enquêteurs ont extrait les métadonnées de photos de l'action publiées en ligne, dont le nom et numéro de série d'un appareil photo[18]. Cela les a aidé à identifier une personne qu'ils ont accusé d'avoir pris les photos.

Affaire de l'association de malfaiteurs de Bure (#2) : Les enquêteurs ont consulté une page Facebook associée à la lutte contre Cigéo et ont ensuite analysé les profils Facebook de toutes les personnes qui avaient « liké » la page[13].

4.15. Patrouilles de police

Utilisée par les tactiques : **Arrestation (p. 15)**, **Dissuasion (p. 15)**, **Incrimination (p. 15)**

Les patrouilles de police sont la pratique de la police de traverser une zone donnée pour la surveiller et la sécuriser. La police peut effectuer des patrouilles soit dans le cadre d'opérations de routine soit en réponse à une menace perçue dans une zone donnée.

Moyens de transport

Les patrouilles de police peuvent utiliser différents moyens de transport :

- Des véhicules sérigraphiés ou banalisés.
- Le déplacement à pied.
- Des **hélicoptères, drones et avions de surveillance (p. 47)**.

Patrouilles de routine

Les patrouilles de police de routine se font généralement dans des périmètres étendus autour des commissariats. Elles servent à établir une présence policière visible pour dissuader des criminels potentiels, et parfois à prendre des criminels malchanceux « la main dans le sac ».

Patrouilles en réponse à une menace

Si la police est avertie d'une menace dans une zone donnée qu'elle juge digne d'être investiguée, elle enverra une ou plusieurs patrouilles. Le temps entre le moment où la police est avertie de la menace et l'arrivée des patrouilles dépend de la distance entre la zone à investiguer et l'unité de police disponible la plus proche. La police peut être avertie d'une menace par :

- Une patrouille de routine qui tombe sur la menace par hasard.
- Des **vigiles (p. 52)** ou des **civils (p. 39)**.
- Un **système d'alarme (p. 50)** (par exemple des détecteurs de mouvement dans un bâtiment), soit directement soit via une entreprise de sécurité qui s'occupe du système d'alarme.
- Des policiers surveillant des **images de vidéosurveillance (p. 41)** en temps réel.
- Un·e **infiltré·e (p. 27)** ou un·e **indic (p. 26)**.

Mesures d'atténuation

Attaque (#2) : La police peut perturber une action. Pour contrer ça, tu peux les distraire en lançant une attaque quasi-simultanée à l'autre bout du quartier, ou en interrompant leurs communications en incendiant l'antenne téléphonique utilisée pour les communications de la police.

La police peut te suivre après une action. Pour contrer ça, tu peux utiliser des techniques pour les arrêter ou les ralentir, soit préventivement soit pendant une poursuite : hérissons ou herses, coups de feu, barricades, pierres, feux d'artifice, etc.

Préparation minutieuse de l'action (#2) : Tu peux préparer minutieusement une action pour prendre en compte le risque de patrouilles de police de routine interférant avec l'action, un risque qui est toujours présent, sauf peut-être dans des zones reculées.

Reconnaissance (#2) : Avant une action, tu peux identifier le commissariat le plus proche, les horaires de rotation des équipes, et les itinéraires des patrouilles, et tu peux identifier des itinéraires qui ne sont pas visibles de patrouilles de police et qui compliqueraient une poursuite (forêts, voies de chemin de fer, etc.)

[46]https://notrace.how/resources/fr/#monica-francisco

Frapper aux portes c'est quand un adversaire vient frapper là où tu habites pour t'intimider ou pour obtenir des informations. Frapper aux portes vise à intimider ou créer de la paranoia, à voir qui est suceptible de parler et potentiellement d'être recruté comme **indic (p. 26)**, et à obtenir des informations grâce aux personnes qui parlent.

En prenant note des personnes que tu appelles ou à qui tu rends visite après qu'il soit venu frapper chez toi, l'adversaire peut **cartographier ton réseau (p. 16)**.

Dans de nombreux pays, il est plus facile pour l'État de frapper aux portes que de faire des **perquisitions (p. 30)** car frapper aux portes ne demande pas de mandat ou autre autorisation légale.

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques pour que ce soit plus difficile pour un adversaire de prendre note de qui tu contactes après qu'il ait frappé à ta porte.

Éviter l'auto-incrimination (#2) : Si un adversaire frappe à ta porte, tu peux éviter de lui parler : à la place, préviens tes réseaux et envisage de t'exprimer publiquement sur la situation.

Opérations répressives

Scintilla (#2) : En mai 2019, des policiers ont toqué à la porte de Boba sous le prétexte de devoir dire quelque chose à une autre personne[38]. Cependant, une fois à l'intérieur, ils ont révélé un mandat d'arrêt au nom de Boba, l'ont arrêté, et ont perquisitionné la maison.

4.11. Indics

Utilisée par les tactiques : **Incrimination (p. 15)**

Un·e indic (ou *balance*) est une personne de l'intérieur d'un réseau qui est recrutée par un adversaire pour fournir des informations sur le réseau.

Un·e indic peut être utilisé·e par un adversaire pour obtenir des preuves ou **cartographier un réseau (p. 16)**.

Il y a plusieurs stratégies de recrutement différentes : cibler des personnes à la périphérie d'un réseau qui sont moins impliquées, des peronnes qui risquent d'être expulsées du pays si elles ne coopèrent pas, des personnes qui ont été accusées d'un autre crime et se voient offrir l'immunité ou la clémence en échange de leur coopération, des personnes qui ne sont plus dans un réseau et ont de la rancœur, des personnes qui font passer l'argent avant la dignité, etc.

Les indics recruté·e·s par l'État sont souvent qualifié·e·s de « sources confidentielles » lors des procès.

Voir le sujet « Infiltré·e·s et indics »[39].

Mesures d'atténuation

Attaque (#2) : Tu peux attaquer des indics quand iels sont découvert·e·s ou des années plus tard pour décourager d'autres personnes de devenir indics.

Dessiner une carte de son réseau (#2) : Tu peux dessiner une carte de ton réseau pour t'assurer que ton réseau ne place pas sa confiance dans des personnes qui pourraient être ou devenir des indics.

Principe du *need-to-know* (#2) : Tu peux appliquer le principe du *need-to-know* pour limiter les informations qu'un·e potentiel·le indic peut obtenir à propos de ton implication dans des actions (si un·e indic n'est pas impliqué·e dans une action, iel ne devrait pas savoir qui est impliqué même si c'est son propre colocataire).

Recherches sur le passé d'une personne (#2) : Tu peux faire des recherches sur le passé d'une personne pour t'assurer qu'une personne de ton réseau n'est pas un·e indic.

Soutien aux prisonnièr·e·s (#2) : Tu peux soutenir des prisonnièr·e·s de tes réseaux : au-delà de l'impératif éthique de ce soutien, les gens ont également moins de chances de devenir des indics s'ils se sentent soutenus et connectés aux mouvements pour lesquels ils ont risqué leur liberté.

Opérations répressives

Opération contre Marius Mason (#2) : La principale preuve contre Marius Mason a été fournie aux enquêteurs par son ex-mari, Frank Ambrose, qui avait participé à certaines des actions avec lui[40]. Frank Ambrose est devenu un indic après son arrestation en 2007 (il a

[38]https://macerie.org/index.php/2019/05/23/incendio-al-carcere-boba-arrestato

[39]https://notrace.how/resources/fr/#topic=infiltrators-and-informants

[40]https://supportmariusmason.org/about-marius/about-the-case

jeté du matériel incriminant dans une poubelle, ce qui a mené à son arrestation)[41]. Pendant plusieurs mois, la balance a amplement collaboré avec le Federal Bureau of Investigation (FBI), enregistrant secrètement 178 conversations téléphoniques et réunions en face-à-face, et fournissant des informations sur 15 personnes[42].

4.12. Infiltré·e·s

Utilisée par les tactiques : **Incrimination (p. 15)**

Un·e infiltré·e est une personne qui infiltre un groupe ou un réseau en se faisant passer pour quelqu'un qu'iel n'est pas afin d'obtenir des informations ou de déstabiliser le groupe ou réseau. Iel peut provenir des rangs de la police, du renseignement ou de l'armée, d'une entreprise ou sous-traitant privé, ou peut agir pour des raisons idéologiques ou sous contrainte (par exemple on lui dit qu'iel sera emprisonné·e s'iel ne travaille pas comme infiltré·e).

Arrêtons de chasser les moutons[43] distingue cinq types d'infiltré·e·s de base :

1. Le poireau : Moins actif, se rend aux réunions et évènements, collecte des documents, observe et écoute.
2. Le dormant : Peu actif au début, plus actif ensuite.
3. Le novice : Faible analyse politique, « aidant », bâtit la confiance qu'on lui accorde et sa crédibilité sur le long terme.
4. Le super activiste : Surgit de nulle part mais rapidement présent partout. Rejoint de nombreux groupes ou comités. Organisateur.
5. L'ultra-militant : Prône des actions militantes et de la conflictualité. (Une variante, l'agent provocateur : incite à des activités illégales risquées ou très clivantes pour provoquer des arrestations ou discréditer un groupe ou un mouvement.)

L'infiltration peut être « superficielle » ou « profonde ». Un·e infiltré·e superficiel·le peut avoir une fausse identité, mais il est plus probable qu'iel retourne à sa vie normale le week-end. L'infiltration superficielle a généralement lieu plus tôt que l'infitration profonde dans le cycle de vie du renseignement, quand les cibles sont encore en train d'être identifiées. Par contraste, un·e infiltré·e profond·e assume son rôle 24 heures sur 24 sur de longues périodes (avec des pauses de temps en temps). Iel peut avoir un travail, un appartement, un·e partenaire, ou même une famille dans le cadre de son rôle d'infiltré·e. Iel aura de faux papiers d'identité officiels, des contrats de travail et de location, etc.

Voir le sujet « Infiltré·e·s et indics »[39].

Mesures d'atténuation

Attaque (#2) : Tu peux attaquer des infiltré·e·s quand iels sont découvert·e·s ou des années plus tard[44] pour décourager la pratique—les policiers infiltrés seront sans doute moins enthousiastes s'il y a un précédent local de violence à leur encontre.

Dessiner une carte de son réseau (#2) : Tu peux dessiner une carte de ton réseau pour rendre ton réseau plus résilient face aux tentatives d'infiltration.

Principe du *need-to-know* (#2) : Tu peux appliquer le principe du *need-to-know* pour limiter les informations qu'un·e potentiel·le infiltré·e peut obtenir à propos de ton implication dans des actions (si un·e infiltré·e n'est pas impliqué·e dans une action, iel ne devrait pas savoir qui est impliqué même si c'est son propre colocataire).

Recherches sur le passé d'une personne (#2) : Tu peux faire des recherches sur le passé d'une personne pour t'assurer qu'une personne de ton réseau n'est pas un·e infiltré·e.

Opérations répressives

Fenix (#2) : Deux policiers ont infiltré le réseau des accusé·e·s pendant plusieurs mois[45]. Durant leur infiltration, les deux policiers :

- Ont essayé de convaincre des personnes de mener des actions plus « radicales », vraisemblablement pour les pousser à commettre des crimes dont elles pourraient par la suite être accusées.
- Ont apporté un soutien matériel actif au réseau (par exemple en imprimant des affiches, en fournissant un moyen de transport et en payant pour l'essence), vraisemblablement pour être bien vus par les gens.

[41] https://www.mlive.com/news/ann-arbor/2008/10/activist_turned_informant_sent.html

[42] https://animalliberationpressoffice.org/NAALPO/snitches

[43] https://notrace.how/resources/fr/#arretons-de-chasser

[44] https://actforfree.noblogs.org/post/2022/03/12/hamburgermany-incendiary-attack-on-the-car-of-former-police-spy-astrid-oppermann

[45] https://antifenix.noblogs.org/post/2015/07/01/the-czech-undercover-police-agents-reveald

4.13. Interprétation biaisée des preuves

Utilisée par les tactiques : **Incrimination (p. 15)**

L'interprétation biaisée des preuves est la pratique qui consiste à interpréter des preuves en faveur d'un point de vue particulier.

L'interprétation biaisée des preuves est la pratique standard des systèmes de justice modernes qui tendent à favoriser les riches et puissants et à discriminer les anarchistes et autres rebelles. Les preuves sont interprétées de manière biaisée à tous les niveaux : lorsqu'elles sont rassemblées par les enquêteurs, présentées par les procureurs, et prises en considération par les juges. Toute information (même banale) peut être utilisée pour construire un récit correspondant aux objectifs d'une enquête.

Mesures d'atténuation

Bonnes pratiques numériques (#2) : Tu peux adopter de bonnes pratiques numériques pour limiter les informations qu'un adversaire a à propos de toi, et donc limiter les informations qu'il peut interpréter de manière biaisée.

Principe du *need-to-know* (#2) : Tu peux appliquer le principe du *need-to-know* pour limiter les informations qu'un adversaire a à propos de toi, et donc limiter les informations qu'il peut interpréter de manière biaisée.

Opérations répressives

Affaire du 8 décembre (#2) : L'affaire a été caractérisée par une absence de preuves que les inculpé·e·s planifiaient une attaque spécifique, et s'est à la place construite autour de l'interprétation de preuves circonstancielles. Voici des exemples de cette interprétation[37] :

- Libre Flot a acquis de l'expérience de combat au Rojava, ce qui a été interprété comme une tentative d'acquérir de l'expérience pour mener des actions en France.
- Libre Float a volé de l'engrais à un magasin, dans l'intention de l'utiliser pour fabriquer de petits explosifs. Le vol a été interprété comme une tentative d'obtenir de l'engrais sans laisser de traces.
- À deux reprises, certain·e·s des inculpé·e·s ont fabriqué des petits explosifs à partir de produits d'entretien ou agricoles, et les ont fait exploser dans des zones isolées où les explosions ne feraient pas de dégâts, ce qui a été interprété comme des tests pour de possibles futures attaques (malgré les affirmations des inculpé·e·s qu'iels faisaient ça juste pour s'amuser).
- Certain·e·s des inculpé·e·s ont fait des parties d'airsoft, qui ont été interprétées comme des entraînements paramilitaires.
- Des notes manuscrites d'un·e des inculpé·e·s contenaient des termes et phrases comme « armes », « recrutement », « nettoyage ADN », « objet incendiaire » et « est-ce qu'on est prêt à ce qu'un camarade soit blessé ou tué ? », qui ont été interprétées comme révélatrices de la volonté de l'inculpé·e de planifier une attaque en France (malgré les affirmations de l'inculpé·e que les notes parlaient soit d'airsoft soit du Rojava).
- Dans des conversations privées, certain·e·s des inculpé·e·s ont fait des commentaires légers ou des fanfaronnades comme « j'ai envie de cramer toutes les banques, tous les keufs » et « si un membre des forces de l'ordre était par terre, moi franchement je l'achève », qui ont été interprétés comme révélateurs de leurs intentions violentes.
- Les inculpé.e.s utilisaient des outils de communication numérique sécurisés, ce qui été interprété comme révélateur de « comportements clandestins ».

4.14. Open-source intelligence

Utilisée par les tactiques : **Incrimination (p. 15)**

L'open-source intelligence (OSINT) est la collecte et l'analyse de données provenant de sources ouvertes (réseaux sociaux, médias traditionnels, blogs, forums, archives publiques…).

Mesures d'atténuation

Éviter l'auto-incrimination (#2) : Un adversaire peut utiliser l'open-source intelligence pour collecter des informations que tu publies volontairement. Pour contrer ça, tu peux éviter d'utiliser des réseaux sociaux et généralement éviter de rendre publiques des informations à propos de toi ou de tes réseaux.