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 2/5

Techniques A–P

Bibliothèque de menaces
Partie 1/5 : Tutoriel, Tactiques
Partie 2/5 : Techniques A–P
Partie 3/5 : Techniques S–V
Partie 4/5 : Mesures d'atténuation
Partie 5/5 : Opérations répressives, Pays

Texte d'origine en français

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.

18 avril 2025

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

- 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.

Opération contre Direct Action (#5) : Dans une perquisition de la maison où vivaient quatre membres de Direct Action, les enquêteurs ont trouvé :[52]

- À propos de l'attaque à l'explosif contre le poste électrique : des plans du lieu de l'action, une copie du communiqué de revendication envoyé après l'attaque, et des coupures de journaux d'articles à propos de l'attaque.
- À propos de l'attaque à l'explosif contre Litton Industries : des photos et des plans du lieu de l'action, des coupures de journaux d'articles à propos de l'attaque, et un canif qu'un membre de Direct Action avait pris dans le fourgon volé utilisé dans l'attaque.

Affaire du 8 décembre (#5) : Pendant les perquisitions, les enquêteurs ont trouvé des armes à feu et des produits pouvant servir à fabriquer des explosifs.[34]

[52] https://web.archive.org/web/20100715145801/http://uniset.ca/other/cs5/27CCC3d142.html

Répression du sabotage de l'usine Lafarge (#5) : 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 (#5) : 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.
- Plusieurs supports de stockage non chiffrés qui contenaient des documents suspects.

Opération contre Louna (#5) : Les enquêteurs ont perquisitionné :

- Le domicile du propriétaire de la voiture qui a amené Louna à l'hôpital.[5] Lors de la perquisition, ils ont saisi la voiture.
- Le domicile d'une personne suspectée d'être visible sur les images de vidéosurveillance de l'hôpital transportant un arrosoir, dans l'espoir de trouver l'arrosoir lors de la perquisition et de confirmer que la personne était bien à l'hôpital.[12]

Opération contre Jeff Luers (#5) : 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 (#5) : Pendant les perquisitions, les enquêteurs ont trouvé :[5]

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

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

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

Sommaire

4. Techniques

4.1. Augmentation de la présence policière

Utilisée par les tactiques : **Arrestation**, **Dissuasion**

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. 41)** 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 (#3)** avant, pendant et après la manifestation.

Mesures d'atténuation

Attaque (#4) : 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.[1]

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

- 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 (#4) : 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 (#4) : 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 (#4) : 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 (#4) : Tu peux te préparer à la répression pour minimiser l'impact des perquisitions.

Opérations répressives

Scripta Manent (#5) : 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 (#5) : 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]

[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

Opérations répressives

Répression contre Zündlumpen (#5) : Les enquêteurs ont envoyé une patrouille de police devant l'appartement d'une personne chaque nuit à des horaires irréguliers pour vérifier si elle était à son appartement.[9]

4.16. Perquisition

Utilisée par les tactiques : **Arrestation, Incrimination**

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 (#4)** 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. 4)**. 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.

Préparation minutieuse de l'action (#4) : 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 (#4)** 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 la tactique : **Incrimination**

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. 34)**.

L'État utilise très fréquemment les listes d'amis sur les réseaux sociaux (une forme d'**open-source intelligence (p. 40)**) pour la cartographie de réseau car cela ne demande pas de mandat ou d'autorisation légale.

Mesures d'atténuation

Bonnes pratiques numériques (#4) : 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 réseaux sociaux et faire que ce soit plus difficile pour un adversaire de cartographier ton réseau.

Cloisonnement (#4) : 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 (#4) : 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 (#4) : 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* (#4) : Tu peux appliquer le principe du *need-to-know* pour que ce soit plus difficile pour un adversaire de cartographier ton réseau.

Téléphones anonymes (#4) : Tu peux utiliser des téléphones anonymes pour que ce soit plus difficile pour un adversaire de cartographier ton réseau.

Éviter l'auto-incrimination (#4) : 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 (#5) : Pour prouver que les accusé·e·s se connaissaient et étaient donc probablement complices, les enquêteurs ont utilisé plusieurs indices :[2]

- Iels avaient été arrêté·e·s aux mêmes manifestations.
- Iels s'appelaient au téléphone régulièrement.

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

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 (#3)** ou des **civils (#3)**.
- Un **système d'alarme (#3)** (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 (#3)** en temps réel.
- Un·e **infiltré·e (p. 36)** ou un·e **indic (p. 34)**.

Mesures d'atténuation

Attaque (#4) : 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 (#4) : 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 (#4) : 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.)

de vidéosurveillance publique ont été trouvées sur les réseaux sociaux.[46]

Répression du sabotage de l'usine Lafarge (#5) : 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.[10] 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 (#5) : 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.[5]

4.15. Patrouilles de police

Utilisée par les tactiques : **Arrestation, Dissuasion, Incrimination**

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 (#3)**.

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 ».

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

- 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, Incrimination**

Un chien policier piste un suspect dans une zone industrielle, aux États-Unis en 2018.

Les chiens de détection sont des chiens entraînés et utilisés par un adversaire pour détecter des odeurs. Les chiens de détection peuvent être utilisés pour détecter des substances comme des explosifs ou des drogues, pister des personnes, et prendre part à des tapissages olfactifs pour déterminer si l'odeur d'une personne est présente sur un objet.

Une odeur est causée par des composés chimiques volatiles émis par une substance. Par exemple, l'odeur d'un vieux livre est causée par les composés chimiques libérés dans l'air par ses pages, qui se décomposent en permanence.

L'odeur des corps humains est causée par des composés chimiques émis par des sécrétions d'eau (sueur), des sécrétions grasses (sébum), des peaux mortes, et des orifices corporels (bouche, nez, etc.) Chaque personne a une odeur relativement unique qui est relativement stable au fil du temps.

Le sens de l'odorat des chiens est bien plus complexe et développé que celui des humains. Les chiens peuvent :

- Détecter des odeurs très légères.
- Détecter une seule odeur dans un mélange d'odeurs.
- Identifier la direction dont provient une odeur.
- Percevoir l'intensité des odeurs avec une grande précision. Cela peut leur permettre, par exemple, si deux odeurs ont été laissées dans des conditions similaires, de déterminer laquelle des deux odeurs est la plus intense, et donc la plus récente.

Détecter des substances

Un adversaire peut entraîner des chiens de détection à détecter les odeurs émises par des substances comme des explosifs, des drogues, des accélérants, ou, moins couramment, des appareils électroniques. L'adversaire peut utiliser des chiens de détection :

- Sur le lieu d'une action ou pendant une **perquisition (p. 43)** ou une **visite discrète de domicile (#3)** pour déterminer si une substance est présente et la localiser.
- Pendant une **vérification d'identité (#3)** pour déterminer si la personne dont l'identité est en train d'être vérifiée transporte ou a été en contact avec une substance.

Dans de nombreux pays, l'État utilise des chiens de détection pour détecter des substances illégales aux frontières, dans les aéroports, gares, etc.

Pister des personnes

Quand une personne se déplace à pied, elle laisse derrière elle une piste odorante composée de :

- Son odeur, y compris les odeurs émises par les sécrétions d'eau (sueur) et les sécrétions grasses (sébum) de ses pieds et par les peaux mortes qui tombent de son corps. Les odeurs de sueur et de sébum pénètrent les chaussures, y compris les chaussures en caoutchouc.

- 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 la tactique : **Incrimination**

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 (#4) : 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.

Opérations répressives

Opération de 2019-2020 contre Mónica et Francisco (#5) : Les photos utilisées pour identifier Mónica and Francisco sur les images

sants 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 (#4) : 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* (#4) : 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 (#5) : 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 :[34]

- 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).

- Les odeurs des choses collées aux plantes de ses pieds ou aux semelles de ses chaussures.
- Si elle porte des vêtements : les odeurs des particules qui se détachent de ses vêtements.
- Si elle porte des chaussures : les odeurs des matières donc les chaussures sont faites (caoutchouc, cuir, etc.)
- Si elle écrase et casse des plantes vivantes, y compris de l'herbe : les odeurs de sève libérées par les plantes et les odeurs de bactéries décomposant les parties mortes des plantes.
- Si elle écrase et tue des insectes ou autres petits animaux : les odeurs des animaux morts.

Un adversaire peut entraîner des chiens de détection à suivre une telle piste odorante. Il y a deux méthodes de pistage :

- Première méthode : On fournit au chien une odeur, par example sous la forme d'un vêtement porté par un·e suspect·e, et on lui demande de localiser et de suivre une piste qui contient l'odeur. Cette méthode est plus fiable.
- Deuxième méthode : On demande au chien de localiser et de suivre une piste sans lui fournir une odeur. Cette méthode est moins fiable.

Dans de nombreux pays, l'État utilise des chiens de détection pour pister des suspect·e·s, mais parce que les chiens ne sont pas considérés comme fiables, le résultat du pistage n'est pas une preuve solide lors d'un procès. Dans certains pays, le résultat d'un pistage par la première méthode est considéré comme une preuve solide, mais pas le résultat d'un pistage par la deuxième méthode.

Les chiens de détection peuvent souvent suivre une piste odorante jusqu'à deux ou trois jours après qu'elle ait été laissée, ou même, en fonction de divers facteurs, jusqu'à deux ou trois mois. Les facteurs qui influencent la capacité d'un chien de détection à suivre une piste longtemps après qu'elle ait été laissée sont notamment :

- L'entraînement du chien et du maître-chien.
- L'activité humaine sur ou près de la piste.
- Le vent. La circulation d'air peut déplacer les composés chimiques volatiles qui constituent une piste.

- Les précipitations. La pluie, la neige, ou la rosée peuvent dissoudre certains des composés chimiques volatiles qui constituent une piste.

Tapissages olfactifs

Un adversaire peut entraîner des chiens de détection à prendre part à des tapissages olfactifs. Pour mettre en place un tapissage olfactif, l'adversaire collecte des échantillons d'odeur d'un·e suspect·e et de quelques autres personnes, typiquement entre 5 et 10, et place les échantillons côte à côte, typiquement dans une pièce vide avec une certaine distance entre deux échantillons. L'adversaire fournit ensuite une odeur au chien et on demande au chien de déterminer si un des échantillons d'odeur correspond à l'odeur, et, si oui, lequel. Typiquement, on fournit au chien un objet prélevé sur le lieu d'une action qu'on suspecte de porter l'odeur du suspect·e : si le chien détermine que l'échantillon d'odeur du suspect·e correspond à l'odeur de l'objet, l'adversaire peut conclure que le suspect·e a été en contact avec l'objet et peut avoir participé à l'action.

Dans les pays où l'État utilise des tapissages olfactifs, le résultat d'un tapissage olfactif n'est souvent pas une preuve solide lors d'un procès.

Mesures d'atténuation

Préparation minutieuse de l'action (#4) : Un adversaire peut utiliser des chiens de détection pour te pister après une action. Pour contrer ça, en quittant le lieu de l'action, tu peux prévoir de :

- Éviter de laisser derrière toi un objet qui porte ton odeur, que l'adversaire pourrait fournir à un chien pour l'aider à te pister.
- Casser ta piste odorante, par exemple en parcourant une distance significative sur un vélo ou en traversant une grande étendue d'eau.

Opérations répressives

Fenix (#5) : Dans l'une des perquisitions, la police a utilisé des chiens

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

Principe du *need-to-know* (#4) : 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 (#4) : 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 (#5) : 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.

4.13. Interprétation biaisée des preuves

Utilisée par la tactique : **Incrimination**

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 puis-

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

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 ».[36]

Mesures d'atténuation

Attaque (#4) : Tu peux attaquer des infiltré·e·s quand iels sont découvert·e·s ou des années plus tard[44] pour décourager la pratique

[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

de détection entraînés à détecter des explosifs.[3]

Répression contre Zündlumpen (#5) : Dans certaines des perquisitions de février 2025, la police a utilisé des chiens de détection pour localiser des appareils électroniques.[4]

Affaire de l'association de malfaiteurs de Bure (#5) : Des chiens de détection ont été utilisés dans l'une des perquisitions.[5]

4.4. Collaboration des fournisseurs de service

Utilisée par la tactique : **Incrimination**

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

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

[4] https://sansnom.noblogs.org/archives/24738

[5] Source non publique.

informations (par exemple des employés du fournisseur de service, des policiers).

- Des fuites de données :[6] 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.

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 les dates des achats.
- À partir d'un objet ou d'une catégorie d'objets : les noms des personnes qui ont acheté l'objet, ainsi que les dates 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.

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

Opération de 2011-2013 contre Jeremy Hammond (#5) : En juin 2011, les enquêteurs ont recruté un acolyte de Jeremy Hammond, Sabu, comme informateur.[40] Pendant plusieurs mois, Sabu a aidé les enquêteurs à monter un dossier contre Jeremy Hammond. En échange de sa collaboration Sabu a reçu une peine clémente : après avoir passé 7 mois en prison (pour un non-respect des conditions de son contrôle judiciaire), il a été condamné à une peine correspondant à celle qu'il avait déjà purgée.[41]

Sabu connaissait l'identité numérique de Jeremy Hammond mais pas son identité réelle. Pour découvrir l'identité réelle de Jeremy Hammond, les enquêteurs ont utilisé des informations qu'il avait partagé à Sabu lors de conversations en ligne, y compris que[42] :

- Il avait été arrêté à l'édition 2004 de la convention du parti républicain, était passé par une prison fédérale et une prison de comté, et était actuellement sous contrôle judiciaire. Les enquêteurs ont pu vérifier tout cela grâce à des fichiers de police.
- Des camarades à lui avaient été arrêté·e·s à une manifestation spécifique. Les enquêteurs ont pu vérifier qu'un·e « acolyte » de Jeremy Hammond était présent·e à la manifestation.
- Il récupérait de la nourriture dans des poubelles. Les enquêteurs l'ont vu prendre de la nourriture dans des poubelles pendant une opération de surveillance physique.

4.12. Infiltré·e·s

Utilisée par la tactique : **Incrimination**

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

[40] https://rollingstone.com/culture/culture-news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-183599

[41] https://www.latimes.com/nation/nationnow/la-na-nn-hacker-sabu-sentenced-20140527-story.html

[42] https://notrace.how/documentation/jeremy-hammond-affidavit.pdf

Mesures d'atténuation

Attaque (#4) : 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 (#4) : 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* (#4) : 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 (#4) : 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 (#4) : 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 (#5) : 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.[37] Frank Ambrose est devenu un indic après son arrestation en 2007 (il a jeté du matériel incriminant dans une poubelle, ce qui a mené à son arrestation).[38] 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.[39]

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

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

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

- 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 (#4)** 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).

Services postaux

Les services postaux peuvent permettre à un adversaire de surveiller ton courrier.

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.

Mesures d'atténuation

Achats anonymes (#4) : 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 (#4) : 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[7] 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[8] 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 (#4) : 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

Opération contre Boris (#5) : 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.

Répression contre Zündlumpen (#5) : Les enquêteurs ont utilisé la collaboration de banques pour :[9]

- Analyser les relevés bancaires d'une éditrice présumée du journal, y compris des relevés bancaires vieux de 8 ans, pour déterminer si la personne avait acheté du matériel d'imprimerie.
- Obtenir, en temps réel, les emplacements des retraits d'espèces faits par une personne qu'ils cherchaient à localiser. Quand un retrait d'espèce avait lieu, les enquêteurs envoyaient une patrouille à l'emplacement du retrait pour essayer de localiser

[7] https://torproject.org/fr
[8] https://riseup.net/en/security/resources/radical-servers
[9] https://notrace.how/resources/fr/#gendarmes-et-voleurs

Éviter l'auto-incrimination (#4) : 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 (#5) : En mai 2019, des policiers ont toqué à la porte de Boba sous le prétexte de devoir dire quelque chose à une autre personne.[35] 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 la tactique : **Incrimination**

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

Un adversaire peut utiliser différentes stratégies pour recruter un·e indic :

- Cibler des personnes qui sont perçues comme plus susceptibles de devenir des indics : des personnes à la périphérie d'un réseau qui sont moins impliquées, des personnes qui ne sont plus dans un groupe ou réseau et ont de la rancœur…
- Menacer quelqu'un de conséquences négatives s'iel ne devient pas un·e indic : une peine de prison plus longue, une expulsion du pays…
- Offrir à quelqu'un des conséquences positives s'iel devient un·e indic : immunité ou clémence dans le dossier judiciaire dans lequel on lui demande de devenir un·e indic ou dans un autre dossier, de l'argent…

Un adversaire peut utiliser un·e indic pour obtenir des preuves ou **cartographier un réseau (p. 4)**.

Voir le sujet « Infiltré·e·s et indics ».[36]

[35] https://macerie.org/index.php/2019/05/23/incendio-al-carcere-boba-arrestato
[36] https://notrace.how/resources/fr/#topic=infiltrators-and-informants

4.10. Frapper aux portes

Utilisée par les tactiques : **Dissuasion**, **Incrimination**

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 susceptible de parler et potentiellement d'être recruté comme **indic (p. 34)**, 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. 4)**.

Dans de nombreux pays, il est plus facile pour l'État de frapper aux portes que de faire des **perquisitions (p. 43)** car frapper aux portes ne demande pas de mandat ou autre autorisation légale.

Mesures d'atténuation

Bonnes pratiques numériques (#4) : 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.

la personne. Cependant, cela n'a pas fonctionné, apparemment parce que la patrouille arrivait toujours trop tard.

- Réduire la limite maximale de retrait d'espèces d'une personne qu'ils voulaient localiser pour la forcer à faire plus de retraits et augmenter les opportunités de la localiser.

Les enquêteurs ont demandé à plusieurs entreprises de fournir des informations sur une personne :

- À des entreprises de vente par correspondance, de fournir les adresses de livraison utilisées par la personne.
- À PayPal, Ebay, et entreprises similaires si la personne avait un compte chez eux, et, si oui, quelles adresses étaient associées au compte.
- À l'entreprise ferroviaire publique allemande (Deutsche Bahn) et l'exploitant d'autobus FlixBus de fournir des informations sur les voyages de la personne.
- À l'ancienne école professionnelle de la personne de fournir la liste des participants aux cours de l'école, vraisemblablement pour identifier de possibles contacts de la personne.

Répression du sabotage de l'usine Lafarge (#5) : 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.[10] 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 (#5) : 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.[11]

Opération contre Louna (#5) : Les enquêteurs ont utilisé la collaboration de l'hôpital pour :

- Apprendre qu'une personne (Louna) était hospitalisée pour des brûlures.[5]

[10] https://notrace.how/resources/fr/#lafarge

[11] https://notrace.how/documentation/case-against-peppy-and-krystal-affidavit.pdf

- Obtenir le dossier médical de Louna.
- Saisir les vêtements de Louna pendant son hospitalisation.[12]
- Obtenir le numéro de téléphone d'un·e proche de Louna, que Louna avait donné à l'hôpital.
- Obtenir les images de vidéosurveillance de l'hôpital.
- Obtenir des informations du système de paiement du parking de l'hôpital.
- Apprendre l'horaire et le lieu d'un rendez-vous de Louna à l'hôpital quelques jours après l'incendie.

Les enquêteurs ont utilisé la collaboration de plusieurs institutions d'État :

- L'Agence nationale des titres sécurisés (ANTS) a fourni des scans de documents d'identité et des dossiers de demandes de documents d'identité.
- Des organismes d'assurance maladie et des mutuelles ont fourni les informations personnelles de personnes sous enquête et de leurs conjoints.
- Le service des impôts a fourni les dossiers d'achat et de vente de maisons des parents et grand-parents de Louna.

Les enquêteurs ont utilisé la collaboration de plusieurs entreprises :

- Des banques ont fourni :
  - Les informations bancaires de plusieurs personnes, y compris de nombreux membres de la famille de Louna.
  - Les adresses IP utilisées pour faire des virements bancaires en ligne.
  - Les emplacements où des personnes ont retiré des espèces.
- Une société d'assurance a fourni l'adresse et la liste des colocataires d'une personne.
- L'opérateur d'autoroutes Vinci a fourni les images de vidéosurveillance de péages d'autoroutes.

[12] https://soutienlouna.noblogs.org/post/2025/01/23/free-louna-des-nouvelles-de-laffaire-de-louna-meuf-trans-anar-incarceree-dans-le-cadre-de-la-lutte-contre-la69

Mesures d'atténuation

Détection d'intrusion physique (#4) : 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 (#5) : Les enquêteurs ont déformé des conversations obtenues grâce à des interceptions téléphoniques pour les rendre suspectes.[33] 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 (#5) : Les enquêteurs ont mal retranscrit ou déformé certaines conversations obtenues par des interceptions téléphoniques ou des microphones cachés pour les rendre suspectes.[34] 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.

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

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

Affaire du 8 décembre (#5) : Une caméra a été installée près d'une petite cabane utilisée par certain·e·s des inculpé·e·s, pointée sur la cabane.[18] Elle a vraisemblablement été installée à environ 10 mètres de la cabane, sur un tronc d'arbre.

4.8. Doxing

Utilisée par la tactique : **Dissuasion**

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. 40)**.

Mesures d'atténuation

Bonnes pratiques numériques (#4) : 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 la tactique : **Incrimination**

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.

- L'entreprise ferroviaire publique française (SNCF) a fourni des informations sur des personnes qui avaient réservé des sièges voisins de personnes sous enquête, y compris leurs photos et informations bancaires.
- Le service de covoiturage BlaBlaCar a fourni des informations sur des personnes qui avaient utilisé le service, y compris leurs photos, informations bancaires, et les trajets effectués.
- Le constructeur automobile Stellantis a fourni les numéros IMSI[13] et IMEI[14] du système de localisation intégré à une voiture. Cependant, les enquêteurs n'ont pas pu localiser la voiture car, pour une raison inconnue, celle-ci n'émettait pas sa localisation.

Les enquêteurs ont demandé à un bailleur social et une agence immobilière de leur fournir les badges d'accès à des résidences.

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont utilisé la collaboration de banques pour obtenir les relevés bancaires d'associations luttant contre Cigéo.[5] 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 :

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

[14] Un numéro International Mobile Equipment Identity (IMEI, identité internationale d'équipement mobile) est un numéro qui identifie un téléphone de manière unique.

- 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[15] 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.
- 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 (#4)**).
- 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 (#3)**, ou grâce à des techniques de corrélation avancées.[16]
- Connaître le numéro IMEI de ton téléphone, qu'il peut trouver en saisissant ton téléphone.

[15]Un numéro International Mobile Equipment Identity (IMEI, *identité internationale d'équipement mobile*) est un numéro qui identifie un téléphone de manière unique.

[16]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.

Cachette ou planque (#4) : 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 (#4) : 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 (#4) : 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 (#4) : Tu peux rechercher des dispositifs de surveillance pour localiser des dispositifs de surveillance cachés vidéo et les retirer.

Opérations répressives

Opération contre Boris (#5) : 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.[17]

Opération contre Louna (#5) : Des caméras ont été installées pour filmer les entrées de plusieurs lieux où habitaient des personnes opposées au projet d'autoroute.[5]

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 (#4)** comme cela s'est produit en Italie où des caméras à détection de mouvement ont été installées pour surveiller une cachette dans une forêt.[32]

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. 4)**.

Voir Ears and Eyes[22] et le sujet « Dispositifs cachés ».[23]

Mesures d'atténuation

Bonnes pratiques numériques (#4) : 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.

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

Mesures d'atténuation

Bonnes pratiques numériques (#4) : 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 :

- Ne pas utiliser de téléphone, ou laisser ton téléphone chez toi.
- Utiliser des applications de messagerie chiffrées de bout-en-bout sur ton téléphone, plutôt que des SMS et appels classiques.

Chiffrement (#4) : 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 (#4) : 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 (#5) : 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.[17] Ils ont fréquemment écouté en temps réel les appels interceptés et utilisé les informations ainsi obtenues pour ajuster des opérations de **surveillance physique (#3)** en cours.

Mauvaises intentions (#5) : 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.[2]

Opération contre Louna (#5) : Les enquêteurs ont utilisé la collaboration des opérateurs de téléphonie mobile pour géolocaliser environ 30 téléphones et intercepter leurs appels, en temps réel.[5] Les enquêteurs ont notamment utilisé les appels interceptés pour :

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

- Entendre parler d'un rendez-vous devant des immeubles résidentiels, mettre en place une surveillance physique de ces immeubles, et arrêter deux personnes s'étant rendues au rendez-vous.
- Entendre Louna prendre rendez-vous avec un médecin, puis contacter le médecin pour obtenir des informations personnelles de Louna, y compris son adresse et son numéro de téléphone.

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont utilisé la collaboration des opérateurs de téléphonie mobile pour :[5]

- 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.

Affaire du 8 décembre (#5) : Les enquêteurs ont utilisé la collaboration des opérateurs de téléphonie mobile pour géolocaliser en temps réel les téléphones des inculpé·e·s et de leurs proches et pour enregistrer des conversations téléphoniques non chiffrées.[18] Notamment :

- Dans un cas, les enquêteurs n'arrivaient pas à déterminer le numéro de téléphone d'un·e des inculpé·e·s, mais avaient déterminé que l'inculpé·e se déplaçait souvent avec une autre personne, donc ils ont géolocalisé en temps réel le téléphone de l'autre personne afin de localiser l'inculpé·e.
- Dans un cas, les enquêteurs suivaient l'un·e des inculpé·e·s dans le cadre d'une opération de **surveillance physique (#3)** mais l'ont perdu·e de vue. Dans l'heure suivante, ils ont géolocalisé

[18] https://soutien812.blackblogs.org/2024/12/15/affaire-du-8-12-analyse-dune-enquete-preliminaire-pnat-et-dgsi

Opérations répressives

Opération contre Boris (#5) : 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.[17]

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.

Opération contre Louna (#5) : Plusieurs balises GPS ont été installées sur des véhicules.[5]

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont caché un dispositif de surveillance par localisation sur un véhicule, qui est resté en place pendant environ un mois.[5]

Affaire du 8 décembre (#5) : Un dispositif de surveillance par localisation a été caché sur un véhicule utilisé par Libre Flot.[18]

4.7.3. Vidéo

Une caméra trouvée derrière le vélux d'une école publique à Berlin, en Allemagne, en juillet 2011.[31]

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

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. 4)**.

Voir Ears and Eyes[22] et le sujet « Dispositifs cachés ».[23]

Mesures d'atténuation

Déplacement en vélo (#4) : Tu peux utiliser un vélo plutôt qu'un autre type de véhicule : contrairement aux autres véhicules, quand tu **recherches des dispositifs de surveillance (#4)** 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 (#4) : 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 (#4) : Tu peux rechercher des dispositifs de surveillance pour localiser des dispositifs de surveillance cachés par localisation et les retirer.

en temps réel le téléphone de l'inculpé·e pour le/la localiser. Ainsi, une heure après avoir perdu l'inculpé·e de vue, les enquêteurs l'ont retrouvé·e et ont repris l'opération de surveillance physique.

4.5. Construction parallèle

Utilisée par la tactique : **Incrimination**

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. 43)** pour saisir le téléphone où ces preuves peuvent être « découvertes » 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, Incrimination**

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 (#5) : 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.[19]

Lors de l'enquête, les policiers italiens ont essayé de cibler une personne vivant en Allemagne.[20] 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 (#5) : Carla a été arrêtée en France grâce à une coopération entre des agences de police et de renseignement italiennes et françaises.[21]

Affaire de l'association de malfaiteurs de Bure (#5) : Certaines des personnes arrêtées avaient participé à des manifestations contre le sommet du G20 à Hambourg, en Allemagne.[5] 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 la tactique : **Incrimination**

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

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

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

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

la journée, les enquêteurs, avec la coopération du propriétaire du café, ont rapidement pris les mesures suivantes :

- Ils ont installé un microphone caché dans une fausse plante à l'intérieur du café.
- Ils ont remplacé un serveur par un opérateur de surveillance qui s'est assuré que le membre de Direct Action et sa copine s'assoient à une table près de la plante.

Affaire du 8 décembre (#5) : Un microphone caché a été installé dans le camion où Libre Flot habitait.[18] Quand l'autorisation légale pour installer et utiliser le microphone a expiré après deux mois, le microphone a été désactivé à distance mais pas retiré du camion. Il a été retiré plusieurs mois plus tard lors des perquisitions.

Un autre microphone caché a été installé dans une petite cabane utilisée par certain·e·s des inculpé·e·s.

4.7.2. Localisation

Une balise GPS retrouvée sous un véhicule à Berlin, en Allemagne, en août 2022.[30]

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

[30] https://notrace.how/earsandeyes/fr/#berlin-2022-08

Recherche de dispositifs de surveillance (#4) : Tu peux rechercher des dispositifs de surveillance pour localiser des dispositifs de surveillance cachés audio et les retirer.

Opérations répressives

Renata (#5) : Six microphones cachés et une caméra ont été retrouvés dans une maison après l'opération.[25] Les microphones ont été retrouvés dans le salon, le couloir, et les chambres. La caméra a été retrouvée dans l'interphone.

Voir le cas Ears and Eyes[26] correspondant.

Opération contre Louna (#5) : Un microphone caché a été installé dans un véhicule.[5]

Scintilla (#5) : 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.[27]

Voir le cas Ears and Eyes[28] correspondant.

Opération contre Direct Action (#5) : Les enquêteurs ont installé des microphones cachés :[29]

- Dans la maison où vivaient quatre membres de Direct Action.
- Dans l'appartement où vivait le cinquième membre de Direct Action.

Un jour, après avoir entendu (vraisemblablement pendant une opération de **surveillance physique (#3)**) qu'un membre de Direct Action et sa copine prévoyaient de déjeuner à un café plus tard dans

[25] https://roundrobin.info/2019/03/trento-sei-microspie-e-una-telecamera-immagini-pesanti

[26] https://notrace.how/earsandeyes/fr/#trento-2019-03

[27] https://macerie.org/index.php/2019/03/12/le-orecchie-della-pedrotta

[28] https://notrace.how/earsandeyes/fr/#torino-2019-03

[29] https://archive.org/details/direct-action-memoirsofan-urban-guerrilla

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 (#4)**) et enlevé par un tiers.

Alimentation électrique

Les dispositifs de surveillance cachés ont besoin d'une alimentation électrique, qui peut être soit une batterie 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.[22]
- Le sujet « Dispositifs cachés ».[23]

4.7.1. Audio

Un microphone trouvé dans un néon à Modène, Italie, en décembre 2015.[24]

[22] https://notrace.how/earsandeyes/fr
[23] https://notrace.how/resources/fr/#topic=hidden-devices
[24] https://notrace.how/earsandeyes/fr/#modena-2015-12

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. 4)**.

Voir Ears and Eyes[22] et le sujet « Dispositifs cachés ».[23]

Mesures d'atténuation

Conversations en extérieur et sans appareils (#4) : 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 (#4) : 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.