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.

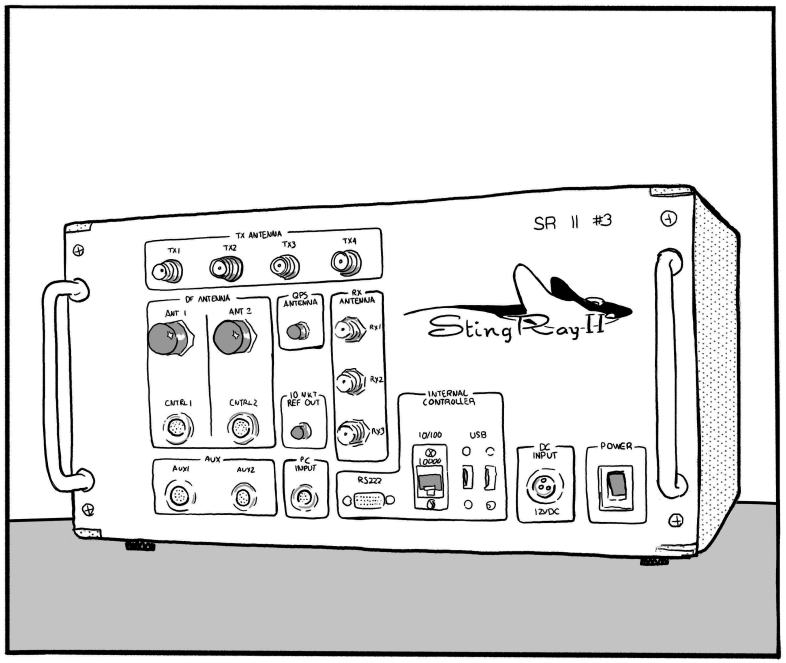
No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

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 3/5

Techniques S–V



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

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

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 faire une visite discrète de ton domicile.

Détection d'intrusion physique (#4) : Tu peux prendre des mesures de détection d'intrusion physique pour détecter une visite discrète de domicile.

Se préparer aux perquisitions (#4) : 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 (#5) : Les enquêteurs ont secrètement fouillé la poubelle devant le domicile de Peppy et Krystal, où ils ont trouvé des documents suspects[39].

Répression du soulèvement de 2019 au Chili (#5) : 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[66].

4.26. Visite discrète de domicile

Utilisée par les tactiques : **Incrimination (#1)**

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 (#2)** dans le domicile.
- Installer des **malware (p. 39)** 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 (#4) : Tu peux garder du matériel d'action qui n'a pas de fonction « légitime » dans une cachette ou une planque,

Sommaire

- 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 (#5) : 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[81]. 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 (#5) : 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[82].

Partisans anarchistes biélorusses (#5) : Les personnes ont été torturées dans les premiers jours de leur détention[83].

Les trois de Varsovie (#5) : Les personnes ont été torturées pendant leur arrestation et les premières heures de leur détention[76].

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

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

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

Mapuches ont neutralisé des vigiles en les désarmant[77], en les ligotant[78] ou en leur tirant dessus[79].

Reconnaissance (#4) : 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 (#1)**, **Incrimination (#1)**

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 :[80].

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

Mesures d'atténuation

Se préparer à la répression (#4) : 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.

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

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

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

[80]

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.

4. Techniques

4.17. Science forensique

Utilisée par les tactiques : **Incrimination (#1)**

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 préle-

vées 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.

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

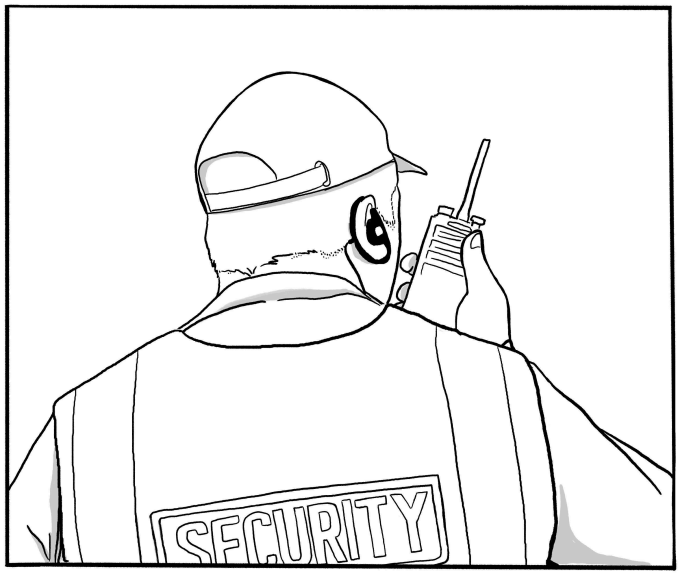
- « blablADN. Tout cramer pour brûler + longtemps : un guide pour ne pas laisser de traces[1] » pour une bonne vue d'ensemble de la science forensique appliquée à l'ADN.
- Le sujet « ADN »[2].

Mesures d'atténuation

[1] https://notrace.how/resources/fr/#blabladn
[2] https://notrace.how/resources/fr/#topic=dna

4.24. Vigiles

Utilisée par les tactiques : **Arrestation (#1)**



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 (#4) : 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

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 (#2)**, 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 (#4) : 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 (#4) : 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 (#5) : 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[4].

Gants (#4) : Tu peux porter des gants pour éviter de laisser de l'ADN sur les surfaces que tu touches.

Protocoles de minimisation de l'ADN (#4) : 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 (#4) : 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 (#4)**.
- 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 (#5) : Des preuves ADN ont été utilisées pour condamner Alfredo Cospito[3].

[3] 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

Opération contre Boris (#5) : 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[4].

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 (#5) : 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[5].

Répression contre Zündlumpen (#5) : 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[6].

Renata (#5) : 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[7]. 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 (#5) : 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[8]. Une personne qui avait refusé de porter un masque s'est faite confisquer des sous-vêtements en garde-à-vue, vraisemblablement pour y prélever son ADN[9].

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

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

[6]https://notrace.how/resources/fr/#chretien-de-baviere

[7]https://roundrobin.info/2020/03/aggiornamenti-su-manu-stecco-juan-e-sasha

[8]https://sansnom.noblogs.org/archives/16831

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

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 (#5) : 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[76]:

- 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.

Affaire du 8 décembre (#5) : En interrogeant les inculpé·e·s en garde-à-vue, les enquêteurs ont[22] :

- 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 (#1)**, **Incrimination (#1)**

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

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

Bonnes pratiques numériques (#4) : Quand tu effectues une cyber-action, tu peux utiliser des techniques d'évasion numérique[74] pour empêcher les systèmes de détection d'intrusion de détecter l'action.

Reconnaissance (#4) : 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 (#1)**

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. 55)**.

Voir Comment la police interroge et comment s'en défendre[75] pour une vue d'ensemble complète des techniques d'interrogatoire de la police.

Mesures d'atténuation

Éviter l'auto-incrimination (#4) : 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 (#5) : En interrogeant des personnes proches de Boris, les enquêteurs ont utilisé des mensonges élaborés pour essayer de les faire parler[4]. Par exemple, les enquêteurs

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

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

Prometeo (#5) : Des traces ADN ont été utilisées pour condamner la personne accusée d'avoir brûlé un DAB[10].

Mauvaises intentions (#5) : 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 (#5) : 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[12]. 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 (#5) : L'accusation contre Peppe était basée sur une correspondance entre des traces ADN trouvées à l'intérieur du colis

[10]https://roundrobin.info/2021/05/sentenza-beppe

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

[12]https://notrace.how/documentation/first-jane-s-revenge-arson-investigation-files.pdf

piégé et son ADN prelevé sur un mégot de cigarette au cours de l'enquête[13].

Affaire de l'association de malfaiteurs de Bure (#5) : Des traces ADN ont été prélevées sur[14] :

- 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 (#5) : 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[15].

[13] https://roundrobin.info/2019/12/verona-una-perquisizione-e-un-arresto

[14] Source non publique.

[15] https://abcsolidaritycell.espivblogs.net/archives/130

4.21. Systèmes d'alarme

Utilisée par les tactiques : **Arrestation (#1)**

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 capteurs peuvent être des détecteurs de mouvement à infrarouge, des capteurs qui détectent l'ouverture des portes, et de nombreux autres types de capteurs[72]. 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[73] 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 (#4) : 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.

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

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

surveillance policière, des policiers l'ont reconnue et se sont mis à la suivre[70]. 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[71]—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 (#2)** 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 (#4) : 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 (#5) : 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].

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

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

Panico (#5) : Des traces ADN étaient la seule preuve contre l'un·e des accusé·e·s[16].

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 (#4) : Tu peux écrire sur des appareils numériques plutôt qu'à la main pour dissimuler ton écriture. En faisant un graffiti, tu peux utiliser uniquement des lettres majuscules et faire des lettres les plus génériques possibles.

Opérations répressives

Scripta Manent (#5) : 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[17].

Opération de 2019-2020 contre Mónica et Francisco (#5) : 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[5]. Les signatures manuscrites sur les étiquettes ont été comparées et correspondaient. Cela a montré que les colis avaient été envoyés par la même personne.

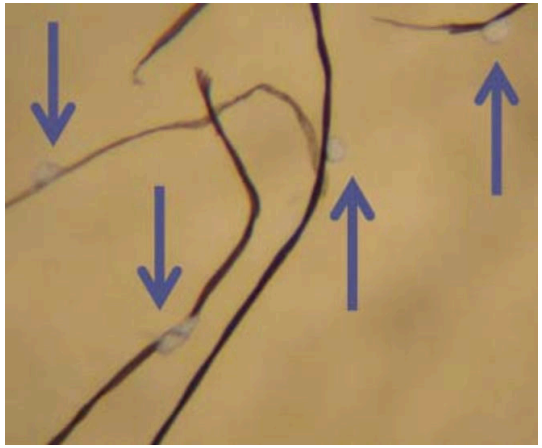
Répression du premier incendie de Jane's Revenge (#5) : Une comparaison entre le graffiti en écriture cursive laissé sur le lieu de

[16]https://panicoanarchico.noblogs.org

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

l'action et des graffitis dans le même style faits quelques mois plus tard lors d'une manifestation ont aidé à identifier la personne[12].

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[18].

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.

[18] *Handbook of Trace Evidence Analysis*[19] (2020), chapitre *Paints and Polymers*.

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

conduisaient vers le lieu de l'incendie[21]. Ils ont garé leur voiture proche du lieu de l'incendie, sous l'oeil de l'équipe de surveillance. Ils sont 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 (#5) : Les enquêteurs[14] :

- 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 (#5) : 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[40]. 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 (#5) : Le jour des arrestations, quand une personne a visité un cybercafé qui était probablement sous

Mesures d'atténuation

Anti-surveillance (#4) : Tu peux faire de l'anti-surveillance pour échapper à une opération de surveillance physique cachée.

Déplacement en vélo (#4) : 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 (#4) : Tu peux faire de la détection de surveillance pour détecter une opération de surveillance physique cachée.

Opérations répressives

Opération contre Boris (#5) : 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[4].

Opération contre Peppy et Krystal (#5) : 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[39]. 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 (#5) : En mars 2020, des policiers ont observé secrètement la personne à une distance d'environ 30 mètres[12]. 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 (#5) : 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

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 »[20].

Mesures d'atténuation

Cachette ou planque (#4) : 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 (#4) : 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 (#4) : 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 (#5) : Lors de la perquisition du garde-meubles, la police a trouvé une pince coupante correspondant aux coupures faites dans la clôture du lieu de la tentative d'incendie de mai[21].

Affaire du 8 décembre (#5) : Pendant les perquisitions, plusieurs objets (gazinière, poêles, gants, spatules) ont été analysés pour y

[20] https://notrace.how/resources/fr/#topic=other-physical-traces
[21] https://www.courtlistener.com/opinion/2627996/state-v-luers

chercher des traces de produits pouvant servir à fabriquer des explosifs[22].

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 (#4) : 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

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

- Une **surveillance aérienne (p. 42)**, 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[67] (*Mesures contre la surveillance*) à propos des principes et techniques de la surveillance physique cachée.
- Maßnahmen gegen Observation[68] (*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 »[69].

[67] https://notrace.how/resources/fr/#surveillance-countermeasures
[68] https://notrace.how/resources/fr/#gegen-observation
[69] https://notrace.how/resources/fr/#topic=physical-surveillance

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.
- 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 (#2)** installé sur le véhicule ou le vélo de la cible.

et des balles anonymement, par exemple grâce à des connexions à des réseaux de crime organisé ou à la fraude.

Cachette ou planque (#4) : 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 »[23].

Mesures d'atténuation

Gants (#4) : Tu peux porter des gants pour éviter de laisser des empreintes digitales sur les surfaces que tu touches.

Préparation minutieuse de l'action (#4) : 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 (#5) : 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

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

lasers. Voir aussi Cinq manières à la portée de tous pour abattre un drone[63].

Détection de surveillance (#4) : 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 (#4) : 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 (#5) : 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[64]. Un texte[65] 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 (#5) : Des drones ont été utilisés pour suivre les émeutièr·e·s qui quittaient les émeutes pour pouvoir les arrêter[66].

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

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

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

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

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. 49)**.
- Améliorer les chances de suivre la cible de la surveillance avec succès lors d'une opération de surveillance **cachée (p. 45)**, 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[59]).
- Localiser des suspects dans le cadre de **patrouilles de police (#2)** 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 seconde, permettant de reconstruire au ralenti presque tout mouvement en extérieur[60], avec des images de haute qualité de nuit[61].

Voir le sujet « Surveillance aérienne »[62].

Mesures d'atténuation

Anti-surveillance (#4) : 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 (#4) : Pendant une manifestation, tu peux abattre des drones avec des feux d'artifice, les pirater, ou les aveugler avec des

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

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

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

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

digitales prélevées ont correspondu à des individus dans le Fichier automatisé des empreintes digitales (FAED)[14].

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 (#2)** sur la scène.

Mesures d'atténuation

Achats anonymes (#4) : 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 (#4) : 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 (#5) : Des traces d'accélérants ont été collectées sur des objets récupérés après des manifestations, et analysées[14].

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 (#2)**, une **visite discrète de domicile (p. 57)** ou une arrestation.

Identification de la voix

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 (#2)**.
- Qui a appelé les autorités pour faire une alerte à la bombe.

Voir aussi

À propos d'identification de l'auteur :

données grâce à la science forensique appliquée aux réseaux informatiques.

Cloisonnement (#4) : 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[26] et en redémarrant entre chaque session.
- Utilisant Qubes OS[57] avec différentes machines virtuelles Whonix[58] que tu n'utilises pas simultanément.

4.20. Surveillance physique

Utilisée par les tactiques : **Incrimination (#1)**

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.

[57] https://qubes-os.org
[58] https://whonix.org

cessite 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 (#2)**, en compromettant ton routeur avec un **malware (p. 39)**, ou en surveillant tes connexions réseau filiaires ou sans fil à partir d'un véhicule de surveillance à proximité de ton domicile.

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[33], 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. 42)** l'observait chez lui pour prouver que le pseudonyme lui appartenait[56].

Mesures d'atténuation

Bonnes pratiques numériques (#4) : Tu peux adopter de bonnes pratiques numériques, et en particulier utiliser Tor[33], pour que ce soit plus difficile pour un adversaire de surveiller et analyser ton traffic réseau.

Chiffrement (#4) : Tu peux chiffrer des données « en mouvement » pour que ce soit plus difficile pour un adversaire d'analyser ces

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

- Counteracting Forensic Linguistics[24] (*Contrer la science forensique appliquée à la linguistique*).
- Qui a écrit ça?[25].

Mesures d'atténuation

Dissimulation biométrique (#4) : Tu peux cacher les propriétés accoustiques de ta voix pour contrer l'identification de la voix.

Masquer son style d'écriture (#4) : Tu peux cacher ton style d'écriture pour contrer l'identification de l'auteur.

Opérations répressives

Scripta Manent (#5) : 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[17].

4.17.8. Numérique

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

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

[25] 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 (#4) : 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[26], 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 (#4)** et accède-y avec Tails[26].

Chiffrement (#4) : 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.

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

Chiffrement (#4) : 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[53].

Cloisonnement (#4) : Si un adversaire installe un malware sur une clé USB Tails[26] ou une machine virtuelle Qubes OS[54] 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 (#5) : Un malware a été installé sur l'ordinateur d'un·e des accusé·e·s[55]. 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 (#5) : Les enquêteurs ont fait cinq requêtes pour installer à distance des logiciels espions[9]. 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 né-

[53]https://forbiddenstories.org/fr/a-propos-du-projet-pegasus

[54]https://www.qubes-os.org

[55]https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy

opérateurs de téléphonie mobile les noms correspondant aux numéros de téléphone[4].

Affaire de l'association de malfaiteurs de Bure (#5) : 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[14].

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[51] 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. 32)** à l'appareil.

Voir le sujet « Logiciels malveillants ciblés »[52].

Mesures d'atténuation

Analyse des ordinateurs et téléphones (#4) : 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 (#4) : 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.

[51] https://fr.wikipedia.org/wiki/Hameçonnage

[52] https://notrace.how/resources/fr/#topic=targeted-malware

Effacement et protection des métadonnées (#4) : 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.

Éviter l'auto-incrimination (#4) : 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 (#4)**).

Opérations répressives

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont analysé des supports de stockage en extrayant automatiquement les fichiers contenant les mots clés suivants en rapport avec l'enquête[14] :

- « 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 caracté-

ristiques 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 (#4) : 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 (#4) : Tu peux porter des vêtements amples pour cacher ta démarche.

Opérations répressives

Bialystok (#5) : 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[27].

Scintilla (#5) : 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[28].

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.

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

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

- 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 »[50].

Mesures d'atténuation

Chiffrement (#4) : 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 (#4) : 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 (#5) : Les enquêteurs ont utilisé des IMSI-catchers lors d'opérations de **surveillance physique (p. 42)** pour trouver les numéros de téléphone de personnes que Boris rencontrait—et ont ensuite identifié ces personnes en demandant aux

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

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[48] et IMEI[49].
- 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 (#2)**.
- Dans le cadre d'une opération de **surveillance physique (p. 42)** 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 :

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

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

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. 27)** peuvent être utilisés pour automatiser le suivi d'individus à travers un espace.

Voir le sujet « Reconnaissance faciale »[29].

Mesures d'atténuation

Dissimulation biométrique (#4) : 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 (#4) : 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 (#5) : 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[5].

Opération de 2013 contre Mónica et Francisco (#5) : La principale preuve contre Mónica et Francisco était une comparaison de photos des deux avec des images de vidéosurveillance publique qui

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

montraient leurs visages découverts alors qu'iels étaient dans le métro, peu avant ou après l'action[30].

4.18. Surveillance de masse

Utilisée par les tactiques : **Dissuasion (#1)**, **Incrimination (#1)**

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 (#4) : 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

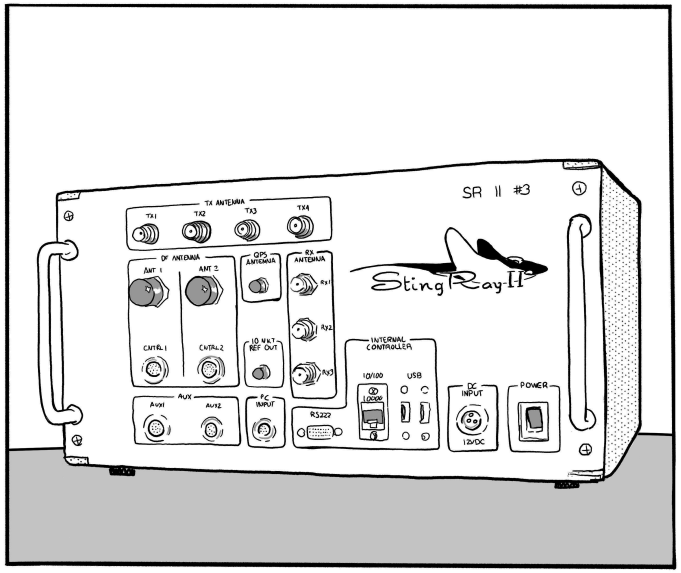
[30]https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf

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 (#5) : Les enquêteurs ont contourné l'authentification de cinq supports de stockage chiffrés trouvés dans des perquisitions[14] :

- 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.

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

Mesures de détection d'accès physique (#4) : Tu peux prendre des mesures de détection d'accès physique pour détecter si un appareil a été **accédé physiquement (p. 32)**.

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.

Recherche de dispositifs de surveillance (#4) : Avant d'entrer un mot de passe dans une pièce où des **dispositifs de surveillance cachés vidéo (#2)** 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 (#5) : 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[47].

Répression du sabotage de l'usine Lafarge (#5) : 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[9] :

- 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

[44] https://debian.org

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

[46] https://grapheneos.org/faq#encryption

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

Opération contre Boris (#5) : 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)[4].

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 (#5) : 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[14].

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.

Mesures d'atténuation

Attaque (#4) : 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 (#4) : 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 gueteu·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 (#4) : 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 (#5) : 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[31].

Opération de 2019-2020 contre Mónica et Francisco (#5) : 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[5].

Partisans anarchistes biélorusses (#5) : 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[14]. 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

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

- 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. 55)**.
- Interception visuelle : observer le propriétaire de l'appareil taper le mot de passe de chiffrement via une **caméra cachée (#2)** ou un·e **infiltré·e (#2)** ou **indic (#2)**.
- 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. 39)** installé à distance ou en **accédant physiquement (p. 32)** à l'appareil.
- Exploiter une faille au niveau de l'implémentation du processus de chiffrement.

Mesures d'atténuation

Bonnes pratiques numériques (#4) : 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[44] et Tails[26], et que le service de police scientifique de la police fédérale allemande n'a pas pu déchiffrer après avoir essayé pendant une année[45].
- 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[46].

- Via un·e **infiltré·e (#2)** ou un·e **indic (#2)** qui a accès à l'appareil.

Mesures d'atténuation

Analyse des ordinateurs et téléphones (#4) : Tu peux faire une analyse des ordinateurs et téléphones pour détecter si un appareil a été accédé physiquement par un adversaire.

Bonnes pratiques numériques (#4) : 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 (#4) : Un adversaire pourrait accéder physiquement à tes appareils numériques via un·e **infiltré·e (#2)** ou un·e **indic (#2)**. 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 (#4) : 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 (#4) : 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 (#4)** 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 :

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 »[32].

Mesures d'atténuation

Bonnes pratiques numériques (#4) : Tu peux adopter de bonnes pratiques numériques pour rendre la surveillance numérique de masse inefficace. Par exemple, tu peux utiliser Tor[33] 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.

[32] https://notrace.how/resources/fr/#topic=digital-surveillance
[33] https://torproject.org/fr

Chiffrement (#4) : Tu peux chiffrer des données « en mouvement » pour empêcher des observateurs à certains endroits du réseau d'analyser ces données.

Éviter l'auto-incrimination (#4) : 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 part pour des raisons mûrement réfléchies (par exemple écrire et envoyer un communiqué de revendication tout en adoptant de **bonnes pratiques numériques (#4)**).

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

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

Voir le sujet « Surveillance numérique »[32].

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[42] 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 (#4)** n'est pas efficace).
- Compromettre l'appareil avec un **malware (p. 39)**.
- Compromettre l'appareil avec un enregistreur de frappes matériel[43].

Un adversaire peut accéder physiquement à un appareil :

- Pendant une **perquisition (#2)** ou une **visite discrète de domicile (p. 57)**.
- Après t'avoir arrêté si tu as l'appareil sur toi.
- Pendant un contrôle aux frontières.

[42] https://fr.wikipedia.org/wiki/Système_embarqué_mobile
[43] https://en.wikipedia.org/wiki/Hardware_keylogger

d'immatriculation de la moto sur laquelle Peppy et Krystal sont arrivés au lieu de la manifestation et en sont partis[39].

Répression du premier incendie de Jane's Revenge (#5) : 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[12].

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont utilisé des images des manifestations, filmées par des caméras de surveillance ou des policiers, pour[14] :

- 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 (#5) : 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[40]. Les policiers ont obtenu les images de vidéosurveillance le matin suivant.

4.19. Surveillance numérique ciblée

Utilisée par les tactiques : **Incrimination (#1)**

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

Des techniques extrêmement avancées existent[41] dans l'arsenal des acteurs étatiques, mais on va se concentrer ici sur les techniques

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

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

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

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. 21)**, sa **démarche (p. 20)**, sa **voix (p. 17)**, 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. 21)**.

Voir aussi

- Pas vue pas prise: contre la vidéo-surveillance[34].
- Les sujets « Vidéosurveillance[35] » et « Lecteurs de plaques d'immatriculation automatisés[36] ».

Mesures d'atténuation

Achats anonymes (#4) : Tu peux faire des achats anonymes pour empêcher un adversaire de t'identifier sur les images de vidéosurveillance de magasins physiques.

[34] https://notrace.how/resources/fr/#pas-vue

[35] https://notrace.how/resources/fr/#topic=video-surveillance

[36] https://notrace.how/resources/fr/#topic=automated-license-plate-readers

Attaque (#4) : Tu peux mettre hors d'usage[37] des caméras de surveillance.

Conversations en extérieur et sans appareils (#4) : 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 (#4) : Si tu es filmé·e par des caméras de surveillance, tu peux :

- Pour contrer la **reconnaissance de démarche (p. 20)**, 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. 21)**, 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 (#4) : 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 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 (#4) : 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 (#4) : Tu peux porter une tenue anonyme pour empêcher un adversaire de t'identifier sur des images de vidéosurveillance.

Opérations répressives

Opération contre Boris (#5) : 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.

[37] https://notrace.how/resources/fr/#detruisons-les-cameras

Opération de 2019-2020 contre Mónica et Francisco (#5) : 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)[5].

Répression du sabotage de l'usine Lafarge (#5) : 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[9]. 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[8]. 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 (#5) : Deux des personnes ont prétendumment 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[38].

Opération de 2013 contre Mónica et Francisco (#5) : Des images de vidéosurveillance publique ont été utilisées pour reconstruire les déplacements de Mónica et Francisco avant et après l'action[30]. Cela a montré qu'iels étaient près du lieu de l'action peu avant l'explosion de l'engin.

Opération contre Peppy et Krystal (#5) : Des images de vidéosurveillance d'un bus ont permis aux enquêteurs d'identifier la plaque

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