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 4/5

Mesures d'atténuation

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

- La tenue civile est une tenue qui paraît normale à porter en public. Elle peut comporter des éléments qui cachent tes caractéristiques corporelles tant que ça ne paraît pas suspect (par exemple une casquette, un masque « Covid »).
- La tenue d'action est une tenue qui cache correctement tes caractéristiques corporelles, comme décrit ci-dessus.

2. Loin du lieu de l'action, enlève ta tenue normale et mets la tenue civile, dans un endroit adapté où il n'y a ni caméras de surveillance ni témoins.
3. Près du lieu de l'action, mets la tenue d'action (dans un endroit adapté).
4. Fais l'action.
5. Près du lieu de l'action, remets la tenue civile (dans un endroit adapté).
6. Loin du lieu de l'action, remets ta tenue normale (dans un endroit adapté).
7. Débarrasse-toi de la tenue civile et de la tenue d'action en toute sécurité.

Le «~black bloc~»

Une forme particulière de tenue anonyme est la tactique du « black bloc », où un grand nombre de personnes s'habillent de manière identique lors d'une manifestation, typiquement en noir, de manière à être indiscernables les unes des autres.

Science forensique > Reconnaissance faciale (#3)
Surveillance de masse > Mouchards civils (#3)
Surveillance de masse > Vidéosurveillance (#3)
Surveillance physique > Aérienne (#3)
Surveillance physique > Visible (#3)

La tenue anonyme est la pratique qui consiste à porter des vêtements dans deux buts : cacher tes caractéristiques corporelles, et t'assurer que les vêtements eux-mêmes ne peuvent pas être utilisés pour t'identifier.

Cacher tes caractéristiques corporelles

Pour cacher tes caractéristiques corporelles, tu peux :

- Pour cacher ton visage : porter un masque qui couvre correctement ton visage, y compris tes sourcils et jusqu'en haut de ton nez.
- Pour cacher le reste de ton corps : porter un t-shirt à manches longues, des gants, un pantalon, et des chaussettes hautes.
- Pour cacher la couleur de ta peau : t'assurer que ta peau n'est pas visible, y compris autour de tes yeux, à la jonction de ton t-shirt et de tes gants, à la jonction de ton pantalon et de tes chaussettes.
- Pour cacher la forme de ton corps et ta démarche : porter des vêtements amples (tu peux aussi cacher ta démarche grâce à la **dissimulation biométrique (p. 30)**).

T\'assurer que les vêtements ne puissent pas être utilisés pour t\'identifier

Pour t'assurer que les vêtements utilisés pendant une action ne puissent pas être utilisés pour t'identifier, tu peux :

1. **Acheter anonymement (p. 3)** deux tenues spécialement pour l'action, une « tenue civile » et une « tenue d'action » :

Sommaire

5. Mesures d'atténuation

5.1. Achats anonymes

Techniques contrées par cette mesure d'atténuation :

Collaboration des fournisseurs de service > Autres (#2)
Science forensique > Balistique (#3)
Science forensique > Incendie volontaire (#3)
Surveillance de masse > Vidéosurveillance (#3)

Les achats anonymes sont la pratique qui consiste à acheter des objets sans associer ton identité à l'achat.

Tu devrais acheter anonymement tout objet que tu prévois d'utiliser pour une action. De cette manière :

- Si un adversaire trouve l'objet sur le lieu de l'action (par exemple un dispositif incendiaire avec retardateur qui n'a pas fonctionné) ou des traces de l'objet (par exemple des traces d'accélérant découvertes par la **science forensique appliquée aux incendies volontaires (#3)**) et découvre où l'objet a été acheté, il ne découvrira pas ton identité.
- Si un adversaire obtient tes relevés bancaires grâce à la **collaboration de ta banque (#2)**, il ne découvrira pas l'achat.

Achats anonymes physiques

Pour acheter un objet anonymement dans un magasin physique :

- Fais l'achat un certain temps avant d'utiliser l'objet (par exemple des semaines ou des mois en avance). De cette manière, si un adversaire trouve l'objet et découvre où il a été acheté, il ne pourra pas te voir sur les images récentes des caméras de vidéosurveillance du magasin ou des alentours.
- Fais l'achat dans un magasin qui n'est pas près de là où tu vis.

Tu peux utiliser des téléphones anonymes pour des projets ou actions sensibles pour lesquels tu es obligé·e d'utiliser un téléphone. À moins que les numéros de téléphone aient besoin d'être stables sur le long terme, tu devrais toujours préférer utiliser des téléphones jetables.

Pour mettre en place et utiliser un téléphone anonyme :

- **Achète anonymement (p. 3)** le téléphone, sa carte SIM, et son abonnement.
- N'allume pas le téléphone près de là où tu vis, parce qu'un adversaire peut obtenir l'historique des positions physiques d'un téléphone avec la **collaboration des opérateurs de téléphonie mobile (#2)**.

Téléphones pseudo-anonymes

Les téléphones pseudo-anonymes sont des téléphones que tu as achetés anonymement mais que tu utilises près de là où tu vis. Ils peuvent contrer la **cartographie de réseau (#2)**—surtout si tous les membres d'un milieu ou réseau les utilisent—mais tu ne devrais pas les utiliser pour des projets ou actions sensibles.

Voir aussi

- Le guide d'AnarSec « Kill the Cop in Your Pocket »[10] (*Tue le flic dans ta poche*) sur les dangers liés à l'utilisation d'un téléphone.
- Les bonnes pratiques pour utiliser un téléphone jetable[61] pour plus d'informations sur les téléphones jetables.

5.32. Tenue anonyme

Techniques contrées par cette mesure d'atténuation :

Science forensique > Autres traces physiques (#3)
Science forensique > Reconnaissance de démarche (#3)

[61] https://notrace.how/resources/fr/#telephone-jetable

5.30. Soutien aux prisonnièr·e·s

Techniques contrées par cette mesure d'atténuation :

Indics (#2)

Le soutien aux prisonnièr·e·s est le processus crucial qui consiste à organiser le soutien matériel, logistique et émotionnel des camarades derrière les barreaux. Au-delà de l'impératif éthique de soutenir nos prisonnièr·e·s, les gens ont également moins de chances de devenir des indics s'ils se sentent soutenus et connectés aux mouvements pour lesquels ils ont risqué leur liberté.

Voici des initiatives courantes de soutien aux prisonnièr·e·s :

- Écrire des lettres.
- Fournir un soutien financier aux prisonnièr·e·s ou à leurs proches.
- Poursuivre les projets ou luttes auxquels les camarades emprisonné·e·s ne peuvent plus participer dans leur situation, et plus généralement témoigner de la solidarité sous des formes qui ont du sens pour les camarades derrière les barreaux.
- Aider des prisonnièr·e·s à s'évader de prison.

5.31. Téléphones anonymes

Techniques contrées par cette mesure d'atténuation :

Cartographie de réseau (#2)

Collaboration des fournisseurs de service > Opérateurs de téléphonie mobile (#2)

Un téléphone anonyme est un téléphone qui n'est pas lié à ton identité. Un téléphone jetable est un téléphone anonyme dont tu te débarasses peu après l'avoir utilisé.

Téléphones anonymes

- Va au magasin en utilisant un moyen de transport anonyme (par exemple un **vélo (p. 24)**), et ne prends pas de téléphone.
- Fais de l'**anti-surveillance (p. 5)** avant d'aller au magasin.
- Revêt un certain niveau de **tenue anonyme (p. 52)** pour être moins reconnaissable—un masque « Covid », une casquette, des vêtements dédiés.
- Paie en espèces.
- Veille à ce que ton interaction avec le/la caissièr·e ne soit pas mémorable.
- Si tu dois acheter plusieurs objets, tu peux les acheter dans des magasins différents, dans différents endroits, à différents moments. C'est particulièrement important si tu achètes des objets qui paraîtraient suspects à acheter ensemble.

Achats anonymes en ligne

Tu peux faire des achats anonymes en ligne avec des cryptomonnaies. Tu devrais soit acquérir les cryptomonnaies anonymement, soit les blanchir suffisamment avant de les utiliser, ce qui peut être compliqué, mais est possible avec des cryptomonnaies comme Monero en utilisant Tails[1].

Voir aussi

Voir Prisma[2] pour plus de détails sur les achats anonymes physiques.

[1] https://anonymousplanet.org/guide.html#your-cryptocurrencies-transactions

[2] https://notrace.how/resources/fr/#prisma

5.2. Analyse des ordinateurs et téléphones

Techniques contrées par cette mesure d'atténuation :

Surveillance numérique ciblée > Accès physique (#3)
Surveillance numérique ciblée > Malware (#3)

L'analyse des ordinateurs et téléphones est une discipline très technique qui vise à déterminer si un ordinateur ou téléphone a été compromis. Les faux négatifs sont courants.

Si tu suspectes que l'un de tes appareils a été compromis et que tu veux en savoir plus sur le possible compromis, tu pourrais demander l'aide de l'organisation à but non lucratif AccessNow[3], en gardant à l'esprit qu'il s'agit d'une organisation légale qui pourrait être forcée de partager avec l'État les données que tu lui transmets.

Voir aussi :

- La page Intégrité de l'appareil[4] sur Privacy Guides.
- Practical Linux Forensics[5] pour une introduction détaillée aux compétences nécessaires à ce type d'analyse sur Linux, la plateforme la plus pertinente pour les anarchistes et autres rebelles.

5.3. Anti-surveillance

Techniques contrées par cette mesure d'atténuation :

Surveillance physique > Aérienne (#3)
Surveillance physique > Cachée (#3)

L'anti-surveillance est la pratique qui consiste à prendre des mesures actives pour échapper à une **opération de surveillance physique mobile (#3)**.

[3]https://accessnow.org/help-fr/?ignorelocale
[4]https://www.privacyguides.org/fr/device-integrity
[5]https://notrace.how/resources/fr/#linux-forensics

5.29. Se préparer aux perquisitions

Techniques contrées par cette mesure d'atténuation :

Perquisition (#2)
Visite discrète de domicile (#3)

Se préparer aux perquisitions est le processus qui consiste à prendre des mesures de précaution pour minimiser l'impact d'une potentielle **perquisition (#2)** ou **visite discrète de domicile (#3)**.

Une mesure de précaution importante est de minimiser la présence de choses que tu ne voudrais pas qu'un adversaire trouve durant une perquisition. En particulier :

- Tu devrais chiffrer tous tes appareils numériques avec le **chiffrement complet du disque (p. 20)**, et les éteindre la nuit ou quand tu n'es pas là pour que le chiffrement soit efficace.
- Tu devrais stocker le matériel utilisé pour des actions qui peut sembler avoir une fonction « légitime » séparément, et dans des endroits cohérents (les gants avec le matériel de ménage, etc.)
- Tu devrais stocker le matériel utilisé pour des actions qui n'a pas de fonction « légitime » dans une **cachette ou une planque (p. 18)**, ou, au pire, le laisser transiter chez toi pendant très peu de temps. Dans la plupart des contextes, nous ne pensons pas qu'il faille éviter de garder des écrits anarchistes chez soi, mais tu devrais éviter de garder des guides particulièrement louches.

De plus, pour détecter si un adversaire a **accédé physiquement (#3)** à un appareil électronique pendant une visite discrète de domicile, tu peux utiliser des **mesures de détection d'accès physique (p. 38)**.

Se préparer à la répression est le processus qui consiste à prendre des mesures de précaution pour minimiser l'impact de la répression. La répression a souvent plus d'impact quand on y est moins préparé. Une telle préparation peut sembler épuisante émotionnellement, mais nous pensons qu'elle nous permet en réalité d'agir plus librement. Se préparer à la répression peut avoir des dimensions pratiques ou psychologiques.

Voici des exemples de préparation pratique :

- S'assurer que tes camarades savent quoi faire si tu te fais arrêter, par exemple en partageant à l'avance les identifiants de connexion de ton adresse email professionnelle ou les clés de chez toi, en prévoyant des personnes pour s'occuper des enfants ou payer ton loyer ou ta caution, etc.
- S'assurer que tes projets peuvent continuer si tu es emprisonné·e, ce qui parfois nécessite simplement de partager un mot de passe à l'avance.
- S'entraîner aux arts martiaux pour être mieux équipé·e pour gérer la violence entre prisonnièr·e·s qui est répandue dans beaucoup de prisons.
- Si la possession de drogues est très criminalisée dans ton contexte, tu peux éviter de toucher aux drogues illégales. Un adversaire étatique peut utiliser des accusations pour détention de drogues pour te mettre la pression sur les crimes qui l'intéressent vraiment.

Voici des exemples de préparation psychologique :

- Discuter de leurs expériences avec des camarades qui ont été ciblé·e·s par la répression, y compris de leurs expériences d'incarcération.
- Une expérience décrite dans l'autobiographie de Claudio Lavazza[60] dans laquelle il s'est enfermé dans une maison à la montagne pendant un mois pour se préparer au risque d'être emprisonné.

[60]https://compasseditions.noblogs.org/post/2020/09/05/my-pestiferous-life-claudio-lavazza

Quand faire de l\'anti-surveillance

Il y a deux, et seulement deux, scénarios dans lesquels tu devrais faire de l'anti-surveillance :

- **Si tu es en chemin vers une activité que tu ne veux pas qu'un adversaire observe, et que tu n'as pas d'indication que tu es en train d'être suivi·e**, tu peux faire de l'anti-surveillance pour échapper à une potentielle opération de surveillance physique qui pourrait être en train de te suivre. Le but de l'anti-surveillance dans ce scénario est de réduire le risque d'être suivi·e au moment de mener l'activité prévue.
- **Si tu as une indication que tu es en train d'être suivi·e, et que tu suspectes que l'opération de surveillance prévoit d'agir avec violence contre toi dans l'immédiat** (par exemple t'arrêter ou t'attaquer), tu peux faire de l'anti-surveillance. Le but de faire de l'anti-surveillance dans ce scénario est d'éviter l'action violente suspectée.

Tu ne devrais pas faire de l'anti-surveillance dans d'autres scénarios parce que :

- Si tu es en chemin vers une activité que tu ne veux pas qu'un adversaire observe, mais que tu as une indication que tu es en train d'être suivi·e, tu ne pourrais pas déterminer de manière définitive que les mesures d'anti-surveillance que tu as prises t'ont permis d'échapper à l'opération de surveillance avec succès. Tu annulerais donc dans tous les cas l'activité prévue, rendant l'anti-surveillance inutile.
- Si tu as une indication que tu es en train d'être suivi·e, mais que tu ne suspectes pas que l'opération de surveillance prévoit d'agir avec violence contre toi dans l'immédiat, faire de l'anti-surveillance pourrait révéler à l'opération de surveillance que tu sais qu'elle te suit, ce qui pourrait pousser l'adversaire à s'adapter et devenir plus discret, ce que tu veux éviter.

Un principe de base

Un principe de base de l'anti-surveillance et que, généralement, une opération de surveillance ne veut vraiment pas être détectée par sa cible, et préférerait perdre sa cible plutôt que de risquer d'être détectée. À cause de ça, la plupart des mesures d'anti-surveillance que tu prends devraient chercher à provoquer l'une de deux situations : soit les opérateurs de surveillance se dévoilent d'une manière que tu peux détecter, soit ils te perdent. Tu devrais rester attentif quand tu prends une mesure d'anti-surveillance, pour pouvoir détecter les opérateurs qui se dévoileraient à cause de la mesure.

Exemples

L'anti-surveillance est une pratique avancée. Avant de faire de l'anti-surveillance, nous te conseillons de te renseigner sur le sujet grâce aux liens à la fin de cette description. Ceci dit, voici des exemples d'anti-surveillance :

- Entrer dans un « angle mort » d'une opération de surveillance, c'est-à-dire un espace dans lequel elle te perd de vue, puis mener une série de manœuvres d'évasion, tout en essayant de détecter des opérateurs de surveillance. Par exemple, si tu es à pied en ville, tu peux entrer un bâtiment public bondé, en sortir rapidement par une porte arrière, puis mener d'autres manœuvres d'évasion. Si tu remarques des personnes se presser pour entrer dans le bâtiment derrière toi, ou te chercher dans la rue après que tu sois sorti·e du bâtiment, elles sont peut-être des opérateurs de surveillance.
- Passer d'une zone dégagée, où une opération de surveillance doit rester loin de toi pour ne pas être détectée, à une zone moins dégagée, où l'opération de surveillance doit se rapprocher de toi pour éviter de te perdre, tout en essayant de détecter des opérateurs de surveillance. Par exemple, si tu es à vélo en campagne, tu peux passer d'une route où tu peux voir loin devant et derrière toi à un petit chemin forestier, puis accélérer, t'enfoncer dans la forêt, et sortir de la

compte les techniques qu'un adversaire peut utiliser contre toi pendant la reconnaissance autant que tu les prends en compte pendant l'action elle-même.

Reconnaissance physique

Voici des exemples de reconnaissance physique :

- Inspecter les itinéraires possibles vers et depuis le lieu de l'action pour choisir quel itinéraire tu pourrais prendre. Par exemple, un bon itinéraire peut être peu couvert par des **caméras de surveillance (#3)** et comporter un endroit adapté pour changer de vêtements avant l'action.
- Inspecter le lieu de l'action lui-même, en cherchant des caméras de surveillance, des **vigiles (#3)**, des **systèmes d'alarme (#3)** et des occasions d'attaquer la cible.

Quand tu fais de la reconnaissance physique, tu peux :

- Faire de l'**anti-surveillance (p. 5)** pour contrer le risque de surveillance physique.
- Porter une **tenue anonyme (p. 52)** pour contrer le risque d'être observé ou filmé.

Reconnaissance numérique

Voici des exemples de reconnaissance numérique :

- Visiter le site web de la cible.
- Inspecter le lieu de l'action sur des cartes en ligne.

En faisant de la reconnaissance numérique, tu devrais adopter de **bonnes pratiques numériques (p. 9)**.

5.28. Se préparer à la répression

Techniques contrées par cette mesure d'atténuation :
Perquisition (#2)
Violence physique (#3)

- Contacter ou rencontrer ses ami·e·s ou des membres de sa famille pour leur poser des questions sur la personne.
- Visiter sa maison ou lieu de travail.
- Vérifier ses documents d'identité ou documents administratifs (contrats de travail ou de location, casier judiciaire, etc.)

Nous conseillons deux approches différentes pour ce type de recherches :

- L'approche consensuelle, mutuelle : Si tu fais déjà confiance à quelqu'un dans une certaine mesure mais que tu aimerais plus lui faire confiance, vous pouvez faire des recherches respectives sur le passé de l'autre.
- L'approche non-consensuelle : Si tu suspectes déjà fortement qu'une personne ment à propos de son identité, tu peux faire des recherches sur son passé sans son consentement pour vérifier tes suspicions.

Pour plus d'informations sur ce type de recherches, voir Assurance, courage, lien, confiance : Une proposition de culture de la sécurité[59].

5.27. Reconnaissance

Techniques contrées par cette mesure d'atténuation :

Patrouilles de police (#2)
Surveillance de masse > Vidéosurveillance (#3)
Systèmes d'alarme (#3)
Vigiles (#3)

La reconnaissance est la collecte d'informations sur la cible d'une action. Elle précède la **préparation de l'action (p. 40)**. Elle peut se faire physiquement (par exemple en se déplaçant jusqu'au lieu de l'action pour l'inspecter) ou numériquement (par exemple en se renseignant sur la cible sur Internet). Tu devrais prendre en

[59]https://notrace.how/resources/fr/#assurance

forêt loin de là où tu y es entré·e, dans un endroit auquel des opérateurs de surveillance ne s'attendraient pas. Si tu remarques des personnes agir de manière étrange quand tu entres ou sors de la forêt, ce sont peut-être des opérateurs de surveillance.

Remarques supplémentaires

Si un adversaire remarque que tu fais de l'anti-surveillance, il pourrait s'adapter et se faire plus discret. En faisant de l'anti-surveillance, tu devrais donc éviter de révéler que tu le fais, si possible.

Voir aussi

- Surveillance Countermeasures[6] (*Mesures contre la surveillance*) à propos des principes et techniques d'anti-surveillance.
- Le sujet « Surveillance physique »[7].
- La mesure d'atténuation connexe **Détection de surveillance (p. 27)**.

5.4. Attaque

Techniques contrées par cette mesure d'atténuation :

Augmentation de la présence policière (#2)
Indics (#2)
Infiltré·e·s (#2)
Patrouilles de police (#2)
Surveillance de masse > Fichiers de police (#3)
Surveillance de masse > Mouchards civils (#3)
Surveillance de masse > Vidéosurveillance (#3)
Surveillance physique > Aérienne (#3)

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

Systèmes d'alarme (#3)
Vigiles (#3)

De nombreuses techniques répressives peuvent être contrées efficacement par une simple maxime : la meilleure défense, c'est l'attaque.

La surveillance numérique de masse est impossible si l'infrastructure d'Internet a été déconnectée par la coupure des câbles de fibre optique. La vidéosurveillance repose non seulement sur sa connectivité au réseau, mais aussi sur des caméras physiques qui sont trop décentralisées pour être protégées efficacement d'actes de sabotage. Un témoin peut être poussé à ne pas témoigner lors d'un procès imminent si la voiture devant chez lui est incendiée pendant son sommeil. Les indics et infiltré·e·s peuvent être intimidé·e·s et attaqué·e·s d'une infinité de façons. Une augmentation de la présence policière à un endroit peut signifier une diminution de la présence policière à un autre endroit. Les laboratoires de police scientifique peuvent partir en fumée. Les communications de la police dépendent d'antennes TETRA[8] et P25[9], et les opérations de police dépendent de l'intégrité de leurs véhicules et de leurs commissariats, et de si les policiers eux-mêmes se sentent en sécurité. Les possibilités d'attaque ne sont limitées que par l'imagination.

5.5. Bonnes pratiques numériques

Techniques contrées par cette mesure d'atténuation :

Cartographie de réseau (#2)
Collaboration des fournisseurs de service > Autres (#2)
Collaboration des fournisseurs de service > Opérateurs de téléphonie mobile (#2)
Dispositifs de surveillance cachés > Vidéo (#2)
Doxing (#2)
Frapper aux portes (#2)

[8]https://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio#Usage
[9]https://en.wikipedia.org/wiki/Project_25

Une technique secondaire pour chercher des dispositifs de surveillance est l'utilisation d'équipement de détection spécialisé. Un tel équipement peut être acheté dans des magasins spécialisés ou sur Internet, et inclut :

- Des détecteurs de fréquences radio, pour détecter des dispositifs en train de transmettre des données sur des fréquences radio au moment de la recherche.
- Des détecteurs de lentilles de caméra pour détecter des caméras.
- De l'équipement professionnel—analyseurs de spectre, détecteurs de jonctions non-linéaires, systèmes d'imagerie thermique—qui peut être plus efficace, mais est très cher et complexe à utiliser.

Voir aussi

Voir Ears and Eyes[58], une base de données de dispositifs de surveillance cachés utilisés contre les anarchistes et autres rebelles.

5.26. Recherches sur le passé d'une personne

Techniques contrées par cette mesure d'atténuation :

Indics (#2)
Infiltré·e·s (#2)

Les recherches sur le passé d'une personne sont utilisées pour vérifier qu'une personne est bien qui elle prétend être. Cela peut aider à s'assurer qu'une personne de ton réseau n'est pas un·e infiltré·e ou un·e indic, et ne ment pas sur son identité pour des raisons malveillantes.

Faire des recherches sur le passé d'une personne peut impliquer :

[58]https://notrace.how/earsandeyes/fr

sitifs dans une zone, tu ne peux pas être sûr·e d'avoir trouvé tous les dispositifs présents dans la zone. L'objectif de la recherche devrait donc être d'empêcher un adversaire de collecter des informations à propos de toi, et pas de considérer qu'une zone ne contient pas de dispositifs de surveillance cachés. Les conversations incriminantes devraient toujours avoir lieu **en extérieur et sans appareils électroniques (p. 23)**.

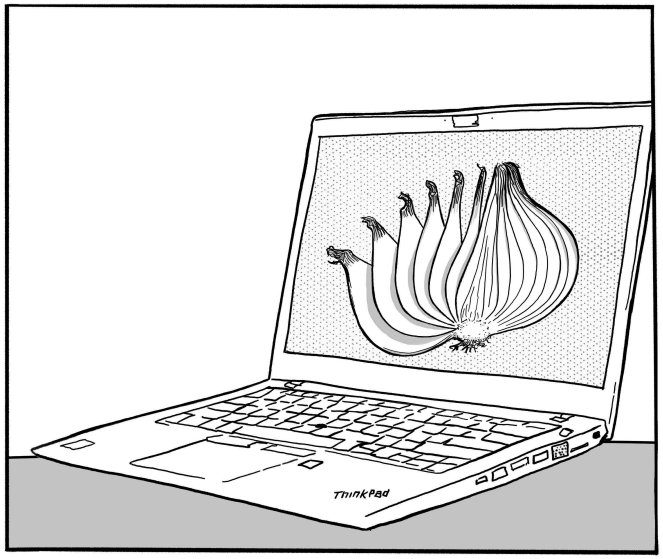
Recherche manuelle, visuelle

La technique principale pour chercher des dispositifs de surveillance est une recherche manuelle, visuelle de la zone :

- Si tu cherches dans un bâtiment, tu peux utiliser des outils appropriés pour démonter les prises électriques, les multiprises, les plafonniers, et autres appareils électroménagers, en cherchant quoi que ce soit qui ne devrait pas se trouver là. Tu peux aussi chercher dans les meubles, en gros tous les endroits où un dispositif de surveillance pourrait rentrer.
- Si tu cherches dans un véhicule, tu peux regarder sous le véhicule, à l'intérieur des roues, sur le pare-chocs arrière, derrière les grilles de ventilation, en cherchant quoi que ce soit qui ne devrait pas se trouver là. Tu peux utiliser des outils appropriés pour démonter l'intérieur du véhicule, le plafond, le tableau de bord, les têtes de siège, et ainsi de suite. Sur des motos et vélos tu peux regarder à l'intérieur ou sous les sièges. Contrairement aux autres véhicules, en cherchant un **vélo (p. 24)** tu peux déterminer avec un haut degré de certitude si un dispositif de surveillance est présent ou non.
- Si tu cherches des caméras installées aux fenêtres de bâtiments dans une rue, tu pourrais les repérer avec des jumelles.
- Si tu cherches des caméras installées à bord de véhicules de surveillance dans une rue, tu peux détecter de tels véhicules grâce à la **détection passive de surveillance (p. 27)**.

Équipement de détection spécialisé

Interprétation biaisée des preuves (#2)
Science forensique > Numérique (#3)
Surveillance de masse > Surveillance numérique de masse (#3)
Surveillance numérique ciblée > Accès physique (#3)
Surveillance numérique ciblée > Contournement de l'authentification (#3)
Surveillance numérique ciblée > Malware (#3)
Surveillance numérique ciblée > Science forensique appliquée aux réseaux informatiques (#3)
Systèmes d'alarme (#3)



La base des bonnes pratiques numériques est de limiter l'emprise de la technologie sur ta vie. Essaie de limiter ton utilisation des appareils numériques, en particulier pour des activités sensibles. Ceci étant dit, il existe un certain nombre de bonnes pratiques que tu peux adopter quand tu utilises des appareils numériques.

N\'utilise pas de téléphone, ou laisse ton téléphone chez toi

Les téléphones sont pistés en permanence, leurs identifiants matériels et les informations liées à l'abonnement téléphonique sont enregistrés par les antennes téléphoniques à chaque connexion, et ils peuvent être piratés. Si possible, n'utilise pas de téléphone. Si tu dois utiliser un téléphone :

- Utilise un smartphone GrapheneOS avec des applications de messagerie chiffrées de bout-en-bout. N'utilise pas les SMS et appels classiques.
- Ne transporte pas le téléphone avec toi, laisse le chez toi en permanence.

Voir le guide d'AnarSec « Kill the Cop in Your Pocket »[10] (*Tue le flic dans ta poche*) sur les dangers liés à l'utilisation d'un téléphone.

Utilise des systèmes d\'exploitation axés sur la sécurité

Utilise :

- Debian[11] ou Qubes OS[12] pour utiliser des ordinateurs au quotidien. Voir le guide d'AnarSec « Qubes OS for Anarchists »[13] (*Qubes OS pour les anarchistes*) sur Qubes OS.
- Tails[14] pour utiliser des ordinateurs pour des choses sensibles, comme lire un article sensible, faire des recherches pour une action, rédiger et envoyer un communiqué de revendication, ou gérer un site web sensible. Voir les guides d'AnarSec « Tails for Anarchists »[15] (*Tails pour les anarchistes*) et « Tails Best Practices »[16] (*Les bonnes pratiques d'utilisation de Tails*).
- GrapheneOS[17] pour les téléphones. Voir le guide d'AnarSec « GrapheneOS for Anarchists »[18] (*GrapheneOS pour les anarchistes*).

[10] https://anarsec.guide/posts/nophones
[11] https://www.debian.org/index.fr.html
[12] https://qubes-os.org
[13] https://anarsec.guide/posts/qubes
[14] https://tails.net/index.fr.html
[15] https://anarsec.guide/posts/tails
[16] https://anarsec.guide/posts/tails-best

- Stocker un objet dans un sac poubelle imperméable neuf, pour que l'ADN présent dans l'environnement ne contamine pas l'objet durant son stockage.
- Détruire les molécules d'ADN avec de l'hypochlorite de soude, qui est présent dans des concentrations appropriées dans certaines marques de Javel.

Voir « blablADN. Tout cramer pour brûler + longtemps : un guide pour ne pas laisser de traces[56] » pour des suggestions de protocoles, et le sujet « ADN »[57].

5.25. Recherche de dispositifs de surveillance

Techniques contrées par cette mesure d'atténuation :
Dispositifs de surveillance cachés > Audio (#2)
Dispositifs de surveillance cachés > Localisation (#2)
Dispositifs de surveillance cachés > Vidéo (#2)
Surveillance numérique ciblée > Contournement de l'authentification (#3)
Surveillance numérique ciblée > IMSI-catcher (#3)

Une recherche de dispositifs de surveillance est le processus actif qui consiste à essayer de détecter la présence de **dispositifs de surveillance cachés (#2)** dans un bâtiment, un véhicule, ou en extérieur. La technique principale de ce processus est une recherche manuelle, visuelle de la zone. Une technique secondaire est l'utilisation d'équipement de détection spécialisé.

Objectif de la recherche

Effectuer une recherche de dispositifs de surveillance qui soit complète et efficace demande des compétences techniques très poussées. Si tu n'as pas ces compétences, en cherchant des dispo-

[56] https://notrace.how/resources/fr/#blabladn
[57] https://notrace.how/resources/fr/#topic=dna

5.24. Protocoles de minimisation de l'ADN

Techniques contrées par cette mesure d'atténuation :

Science forensique > ADN (#3)

Les protocoles de minimisation de l'ADN te permettent de manipuler des objets tout en minimisant la quantité d'**ADN (#3)** que tu laisses dessus. Certains protocoles permettent de ne pas laisser de traces ADN sur un objet en premier lieu. D'autres protocoles permettent de retirer des traces ADN d'un objet en détruisant chimiquement les molécules d'ADN.

Les protocoles de minimisation de l'ADN peuvent impliquer :

- Acheter un objet dans un emballage en plastique individuel, pour que tu ne risques pas de laisser de l'ADN dessus jusqu'à ce que tu ouvres l'emballage.
- Manipuler un objet en portant une paire de gants imperméables neufs (par exemple des gants de vaisselle), pour qu'il n'y ait pas de traces ADN à l'extérieur des gants qui puissent être transférées sur l'objet.

N'utilise pas Windows, MacOS, les iPhones, ou le système Android de base.

Chiffre tes appareils

Active le **chiffrement complet du disque (p. 20)** sur tous tes appareils numériques.

Utilise des mots de passe robustes

La plupart de tes mots de passe (par exemple les mots de passe que tu utilises pour te connecter à des sites web) devraient être générés et stockés dans un gestionnaire de mots de passe—nous conseillons KeePassXC[19]—pour que tu n'aies pas à les retenir ni même à les taper. Ils peuvent être très longs et aléatoires, genre 40 caractères aléatoires. Tu peux générer de tels mots de passe avec KeePassXC (sélectionne l'onglet « Mot de passe » au moment de générer un mot de passe).

Les mots de passe que tu entres au moment où tu démarres tes appareils chiffrés ainsi que le mot de passe de KeePassXC doivent être mémorisés. Nous conseillons d'utiliser des mots de passe Diceware de 5 à 10 mots[20]. Tu peux générer de tels mots de passe avec KeePassXC (sélectionne l'onglet « Phrase de passe »

[17] https://grapheneos.org

[18] https://anarsec.guide/posts/grapheneos

[19] https://keepassxc.org

[20] Si un adversaire accède physiquement à l'un de tes appareils numériques, il peut essayer de deviner son mot de passe via des tentatives d'authentification automatiques et répétées (un processus qu'on appelle « *brute force* »). Il peut aussi copier les données de l'appareil et attendre des années ou des décennies que soient inventées de nouvelles technologies qui permettent de deviner un mot de passe qu'il ne peut pas deviner aujourd'hui. Pour contrer ça, tu devrais utiliser des mots de passe robustes. En supposant que tu utilises les systèmes d'exploitation que nous conseillons, et sur la base de notre connaissance des capacités des adversaires étatiques, nous te conseillons d'utiliser des mots de passe Diceware de :

- 5 mots pour être plus sûr·e *aujourd'hui*.
- 7 mots pour être plus sûr·e *dans un futur proche*.
- 10 mots pour être plus sûr·e *dans un futur lointain*.

au moment de générer un mot de passe) ou avec des dés physiques[21]. Tu devrais utiliser des mots de passe différents pour chacun de tes appareils chiffrés, mais nous te conseillons d'utiliser le même mot de passe pour toutes tes bases de données KeePassXC (pour que tu aies moins de mots de passe à mémoriser).

Par exemple, si tu as un ordinateur portable chiffré, une clé Tails et un téléphone chiffré, tu devras mémoriser 4 mots de passe de 5 à 10 mots (un pour chaque appareil et un pour les bases de données KeePassXC). C'est beaucoup ! Pour t'assurer de ne pas oublier tous ces mots de passe, tu peux :

- Utiliser des techniques de mémorisation, par exemple répéter les mots de passe dans ta tête chaque jour quand tu te réveilles.
- Stocker une copie des mots de passe sur une clé USB que tu gardes dans une cachette hors de chez toi, et qui est chiffrée avec un mot de passe Diceware de 10 mots. Tu ne mémorises pas ce mot de passe de 10 mots, tu le stockes dans les bases de données KeePassXC d'un ou deux camarades de confiance qui adoptent également ces bonnes pratiques numériques. Ainsi, si tu oublies un mot de passe, tu peux demander le mot de passe de 10 mots au camarade de confiance et récupérer la clé USB : tu y trouveras le mot de passe oublié.
- Stocker une copie des mots de passe sur une clé USB que tu gardes dans une cachette hors de chez toi, et qui est chiffrée avec un mot de passe Diceware de 20 mots. Tu ne mémorises pas ce mot de passe de 20 mots, tu le sépares en deux moitiés de 10 mots chacune, tu écris chaque moitié sur un bout de papier, et tu stockes chaque bout de papier dans une cachette différente (pas avec la clé). Ainsi, si tu oublies un mot de passe, tu peux récupérer les deux bouts de papier, reconstruire le mot de passe de 20 mots, et récupérer la clé USB : tu y trouveras le mot de passe oublié.

[21] https://www.eff.org/dice

- Les personnes qui ne sont pas impliquées dans l'action ne devraient pas spéculer à propos de qui est impliqué.
- Les personnes impliquées dans l'action ne devraient pas révéler leur implication aux personnes qui ne sont pas impliquées.
- Les personnes qui ont un rôle spécifique et limité dans l'action n'ont pas forcément besoin de savoir qui d'autre est impliqué en dehors des personnes avec qui elles communiquent directement.

De plus, tout le monde devrait stopper toute violation du principe du *need-to-know* dans des conversations. Par exemple, si tu entends des personnes parler de leur implication dans une action ou spéculer à propos de l'implication d'autrui, dis-leur d'arrêter.

Quand plusieurs groupes de personnes participent à une action, une structure de coordination qui incarne le principe du *need-to-know* est le « conseil de porte-paroles » (« *spokes council* »). Dans cette structure, une ou deux personnes de chaque groupe sont désignées pour participer au conseil de porte-paroles, où elles retrouvent les porte-paroles des autres groupes. Ainsi, les groupes peuvent se coordonner à travers le conseil sans que qui que ce soit ait besoin de connaître toutes les personnes impliquées. Cependant, cette structure court le risque de créer des « goulets d'étranglement » dans la coordination—si une personne est le seul lien entre deux groupes, elle risque de devenir l'unique gardienne de l'accès à la coordination, et la coordination peut devenir impossible si cette personne est arrêtée par un adversaire.

Voir aussi :

- Secrets And Lies[55] à propos des effets que le secret peut avoir à des niveaux individuels et collectifs.
- Le sujet « Culture de la sécurité »[39].

[55] https://notrace.how/resources/fr/#secrets-lies

Quand tu prévois une action, la préparation minutieuse de l'action est le développement soigné et raisonnable du plan de l'action. Elle succède à l'étape de **reconnaissance (p. 47)**.

La préparation minutieuse de l'action doit clarifier le rôle de chaque personne impliquée dans l'action et comment son rôle se combine aux rôles des autres.

Par exemple, quel est le meilleur itinéraire pour aller et revenir du lieu de l'action, et combien de temps est-ce que vous resterez sur le lieu, compte tenu du temps de réaction présumé de l'adversaire ? Ou bien, qu'est-ce qui pourrait interférer avec une éventuelle poursuite sur votre itinéraire de fuite (par exemple, est-ce que l'adversaire devra sortir de son véhicule pour vous suivre à pied) ? Créer un plan d'action est une forme de modélisation de menaces—qu'est-ce qui pourrait mal se passer, quelles mesures d'atténuation est-ce que vous allez implémenter, et comment ? Par exemple, comment est-ce que vous allez faire de l'**anti-surveillance (p. 5)** avant le point de rendez-vous de l'action ?

5.23. Principe du *need-to-know*

Techniques contrées par cette mesure d'atténuation :

Cartographie de réseau (#2)
Indics (#2)
Infiltré·e·s (#2)
Interprétation biaisée des preuves (#2)

Le principe du *need-to-know* affirme que les informations sensibles ne devraient être partagées que lorsque cela est nécessaire, et seulement dans la mesure du nécessaire. Ce principe complique la répression en contrôlant le flux d'informations à travers des réseaux pour les rendre plus opaques de l'extérieur et plus difficiles à perturber.

Par rapport à une action prévue ou passée, le principe du *need-to-know* devrait être appliqué ainsi :

Utilise Tor ou un VPN

Utilise Tor[22] ou un Virtual Private Network (VPN) réputé quand tu utilises Internet. Si tu utilises Tor ou un VPN et qu'un adversaire surveille ta connexion réseau, il est plus difficile pour lui d'obtenir des données sur ton utilisation d'Internet, comme les sites web que tu visites ou ce que tu fais sur ces sites web (il est aussi plus difficile pour lui de te cibler à l'aide de **malware (#3)**).

Cependant, note que Tor et les VPNs ne sont pas équivalents :

- Si tu utilises Tor, c'est *très difficile*, même pour l'État, d'obenir des données sur ton utilisation d'Internet (tant que tu adoptes par ailleurs de bonnes pratiques numériques).
- Si tu utilises un VPN, ça peut être soit difficile soit facile pour l'État d'obtenir des données sur ton utilisation d'Internet, en fonction de ton contexte, des capacités de surveillance de l'État, et du VPN que tu utilises.

Par conséquent :

- Tu devrais utiliser Tor pour toutes tes activités Internet sensibles, et autant que possible pour tes activités Internet non-sensibles.
- Si tu ne peux pas utiliser Tor pour une certaine activité Internet non-sensible (par exemple parce que tu dois utiliser un site web qui bloque Tor), tu peux utiliser un VPN pour ça.
- Tu ne devrais pas utiliser Internet sans Tor ou un VPN.

Tu peux utiliser Tor et un VPN en même temps en te connectant à un VPN *avant* Tor : cela a plusieurs avantages en terme

[22] https://torproject.org/fr

de sécurité[23]. Tu ne devrais pas te connecter à un VPN *après* Tor sauf si tu sais vraiment ce que tu fais[24].

Utilise des applications de messagerie chiffrées de bout-en-bout

Utilise des applications de messagerie chiffrées de bout-en-bout pour toutes tes communications numériques :

- Idéalement, utilise des applications *peer-to-peer* qui protègent les métadonnées comme Cwtch[25] ou Briar[26]. Autrement, utilise des applications qui protègent les métadonnées comme SimpleX[27] ou Signal[28].
- Les emails ne protègent pas les métadonnées et devraient être évités si possible. Si tu dois communiquer par email, utilise le chiffrement PGP et crée une adresse chez un fournisseur de confiance[29].

Voir le guide d'AnarSec « Encrypted Messaging for Anarchists »[30] (*Applications de messagerie chiffrées pour les anarchistes*) pour des recommendations sur les applications de messagerie chiffrées de bout-en-bout.

Fais des sauvegardes de tes données numériques

Fais régulièrement des sauvegardes de tes données numériques, en particulier des données que tu ne veux vraiment pas perdre, comme la base de données de ton gestionnaire de mots de passe.

[23] Si tu te connectes à un VPN avant Tor, il est plus difficile pour l'État de savoir que tu utilises Tor, et il peut être plus difficile pour l'État d'obtenir des données sur ton utilisation d'Internet à travers des attaques avancées comme le *traffic fingerprinting*.

[24] https://privacyguides.org/en/advanced/tor-overview/#safely-connecting-to-tor

[25] https://cwtch.im

[26] https://briarproject.org

[27] https://simplex.chat

[28] https://signal.org

[29] https://riseup.net/en/security/resources/radical-servers

[30] https://anarsec.guide/posts/e2ee

identiques, cela veut dire que l'ordinateur n'a pas été dévissé.

- Plonger des appareils électroniques dans une boîte transparente remplie de petits objets de différentes couleurs (par exemple, moitié cailloux noirs et moitié cailloux blancs) et prendre en photo les côtés de la boîte. Comme un tel mélange forme un motif complexe, ce serait très difficile pour un adversaire de retirer les appareils électroniques sans modifier le motif. Ainsi, quand tu dois retirer les appareils électroniques de la boîte, tu peux prendre de nouvelles photos des côtés de la boîte et les comparer aux photos d'origine : si les motifs formés par le mélange sont identiques, cela veut dire que les appareils électroniques n'ont pas été accédés. Une application systématique de cette technique est de t'assurer qu'un appareil électronique (par exemple un ordinateur portable) est toujours plongé dans une telle boîte quand tu ne l'as pas avec toi.

Voir le guide d'AnarSec « Make Your Electronics Tamper-Evident »[54] (*Détecte les accès physiques à tes appareils électroniques*) sur comment mettre en place des mesures de détection d'accès physique pour des appareils électroniques.

5.22. Préparation minutieuse de l'action

Techniques contrées par cette mesure d'atténuation :

Augmentation de la présence policière (#2)
Chiens de détection (#2)
Patrouilles de police (#2)
Science forensique > ADN (#3)
Science forensique > Autres traces physiques (#3)
Science forensique > Empreintes digitales (#3)
Science forensique > Incendie volontaire (#3)
Surveillance de masse > Mouchards civils (#3)

[54] https://anarsec.guide/posts/tamper

Un mélange de lentilles corail et de lentilles noires qui forme un motif complexe. Des appareils électroniques peuvent être plongés dans le mélange de manière à ce que lorsqu'on y accède, le motif change.

Les mesures de détection d'accès physique sont des mesures de précaution qui permettent de détecter quand quelque chose a été **accédé physiquement (#3)** par un adversaire.

Les mesures de détection d'accès physique peuvent être utilisées :

- Pour détecter si un adversaire a accédé à un appareil électronique pendant une **visite discrète de domicile (#3)** (auquel cas il pourrait avoir installé un **malware (#3)** sur l'appareil).
- Pour détecter si un adversaire a accédé à une **cachette ou une planque (p. 18)**.

Voici des exemples de mesures de détection d'accès physique :

- Mettre du vernis à ongles sur les vis d'un ordinateur portable et prendre les vis en photo. Comme le vernis à ongles forme des motifs complexes, ce serait très difficile pour un adversaire de retirer une vis sans modifier le motif. Ainsi, quand tu veux vérifier que l'ordinateur n'a pas été ouvert, tu peux prendre de nouvelles photos des vis et les comparer aux photos d'origine : si les motifs du vernis à ongles sont

Chiffre tes sauvegardes avec le **chiffrement complet du disque (p. 20)**. Une pratique courante est d'avoir deux sauvegardes :

- Une sauvegarde « sur site » que tu gardes chez toi et que tu mets à jour fréquemment, par exemple une fois par semaine.
- Une sauvegarde « hors-site » que tu gardes hors de chez toi et que tu mets à jour moins fréquemment, par exemple une fois par mois.

L'avantage de la sauvegarde sur site c'est qu'elle a une version plus récente de tes données. L'avantage de la sauvegarde hors-site c'est qu'elle ne peut pas être saisie en cas de **perquisition (#2)** chez toi.

Stocke tes appareils de manière à détecter si ils ont été trafiqués

Si un adversaire accède physiquement à un de tes appareils numériques, il pourrait le trafiquer, de telle sorte qu'il ne soit plus sûr à utiliser. Pour détecter quand un adversaire a accédé physiquement un appareil, tu peux utiliser des **mesures de détection d'accès physique (p. 38)**.

Achète tes appareils anonymement

Acheter des appareils numériques anonymement (p. 3) a deux avantages :

- Si un de tes appareils numériques est saisi par un adversaire, l'adversaire peut récupérer des données de l'appareil grâce à la **science forensique appliquée au numérique (#3)**. Si tu as acheté l'appareil anonymement, l'adversaire ne sera peut-être pas capable de lier l'appareil, et donc les données récupérées, à toi.
- Si tu achètes un appareil numérique d'une manière qui ne te donne pas immédiatement accès à l'appareil (par exemple si tu commandes un ordinateur portable en ligne), acheter anonymement peut empêcher un adversaire qui te cible de

trafiquer l'appareil avant que tu y aies accès (par exemple entre l'achat et la livraison de l'ordinateur portable).

Si nécessaire, détruis physiquement tes supports de stockage

Si tu veux t'assurer qu'un adversaire ne puisse jamais accéder aux données stockées sur un support de stockage (par exemple le disque dur d'un ordinateur portable, une clé USB, une carte SD), la seule solution est de détruire physiquement le support de stockage. En effet :

- Même si le support de stockage est chiffré avec le **chiffrement complet du disque (p. 20)** avec un mot de passe robuste, un adversaire pourrait **contourner le chiffrement (#3)**.
- Les supports de stockage modernes peuvent stocker une copie cachée de leurs données dans des *cellules de mémoire libres*[31], ré-écrire par-dessus tout le support de stockage n'est donc pas suffisant.

Pour détruire physiquement un support de stockage :

- D'abord, formatte et ré-écrit par-dessus tout le support de stockage comme mesure de sécurité supplémentaire.
- Puis utilise un mixeur de bonne qualité ou une disqueuse pour le réduire en petits bouts, idéalement de moins de deux millimètres.

Autres bonnes pratiques

- Le hameçonnage (ou *phishing*) c'est quand un adversaire te piège pour te faire révéler des informations ou installer un **malware (#3)** sur un de tes appareils numériques. Pour contrer ça, n'ouvre pas des fichiers et ne clique pas sur des liens qui te sont envoyés par des personnes à qui tu ne fais

[31] https://tails.net/doc/encryption_and_privacy/secure_deletion/index.fr.html

Masquer son style d'écriture est la pratique qui consiste à altérer la manière dont on écrit pour contrer l'identification de l'auteur par la **science forensique appliquée à la linguistique (#3)**.

Par exemple :

- Tu peux écrire de manière concise et claire.
- Avant de publier un texte, tu peux corriger ses fautes d'orthographe et de grammaire pour t'assurer qu'il ne contienne pas d'erreurs uniques qui pourraient être reliées à toi.
- Pour identifier l'auteur·ice d'un texte, un adversaire peut chercher des échantillons de textes écrits par cette personne pour les comparer au texte. Pour contrer ça, tu peux éviter de garder chez toi des textes que tu as écrits et qui pourraient être trouvés lors d'une **perquisition (#2)** ou d'une **visite discrète de domicile (#3)**, et d'une manière générale éviter de publier des textes en ton nom tout au long de ta vie.

Voir Counteracting Forensic Linguistics[52] (*Contrer la science forensique appliquée à la linguistique*) et Qui a écrit ça?[53].

5.21. Mesures de détection d'accès physique

Techniques contrées par cette mesure d'atténuation :

Surveillance numérique ciblée > Accès physique (#3)

Surveillance numérique ciblée > Contournement de l'authentification (#3)

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

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

Caractéristiques des mains

Pour cacher les caractéristiques de tes mains comme ta couleur de peau ou tes tatouages, porte des gants qui couvrent entièrement ta peau. Voir la mesure d'atténuation connexe **Tenue anonyme (p. 52)**.

Considérations supplémentaires

Quand tu portes des gants, souviens-toi que :

- Tu peux laisser des empreintes digitales à l'intérieur des gants que tu portes, selon leur matière.
- Tu peux laisser de l'ADN à l'intérieur des gants que tu portes.
- Si tu portes des gants pendant une action, des traces du lieu de l'action (par exemple des traces d'accélérant) peuvent se retrouver sur les gants, et des traces des gants (par exemple des fibres textiles) peuvent se retrouver sur le lieu de l'action. Ces traces pourraient être utilisées pour relier les gants au lieu de l'action.

Pour toutes ces raisons, si tu dois utiliser des gants pendant une action, tu devrais utiliser des gants neufs dédiés à l'action et t'en débarrasser après coup.

Voir aussi

- Le sujet « Empreintes digitales »[50].
- Handschuhe[51] (en allemand).

5.20. Masquer son style d'écriture

Techniques contrées par cette mesure d'atténuation :
Science forensique > Linguistique (#3)

[50]https://notrace.how/resources/fr/#topic=fingerprints
[51]https://militanz.blackblogs.org/163-2

pas confiance. Voir le chapitre d'AnarSec « Phishing Awareness »[32] (*Avoir conscience du hameçonnage*) sur les mesures que tu peux prendre contre le hameçonnage.

- Le **doxing (#2)** c'est quand un adversaire publie tes informations personnelles sans ton consentement. Voir Doxcare: Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment[33] (*Doxcare : prévention et soins pour celleux ciblé·e·s par le* doxing *et le harcèlement politique*) sur les mesures que tu peux prendre contre le doxing.

5.6. Cachette ou planque

Techniques contrées par cette mesure d'atténuation :
Dispositifs de surveillance cachés > Vidéo (#2)
Perquisition (#2)
Science forensique > Autres traces physiques (#3)
Science forensique > Balistique (#3)
Visite discrète de domicile (#3)

Les cachettes et les planques sont deux manières de stocker du matériel incriminant. Si du matériel incriminant est stocké dans une cachette ou une planque plutôt que chez toi, il ne sera pas trouvé par un adversaire lors d'une **perquisition (#2)** ou une **visite discrète (#3)** de ton domicile. Une cachette est un endroit caché, souvent en extérieur, sur lequel on a peu de chances de tomber par hasard. Une planque est une maison, appartement, ou autre espace qu'un adversaire ne sait pas que tu utilises.

Les cachettes et les planques ont chacune des avantages et inconvénients :

- Il est plus facile de mettre en place une cachette.
- Il est plus facile de **minimiser les traces ADN (p. 43)** dans une cachette.
- Il est plus facile de changer l'emplacement d'une cachette.

[32]https://anarsec.guide/posts/tails-best/#phishing-awareness
[33]https://notrace.how/resources/fr/#doxcare

- Une planque fournit plus d'espace de stockage et peut être utilisée pour d'autres choses que le stockage, par exemple pour dormir, préparer du matériel, etc.

Voici des exemples de cachettes :

- Une boîte enterrée dans une zone boisée loin des sentiers (pour que les promeneurs ne risquent pas de tomber dessus).
- Un endroit caché dans un bâtiment abandonné un peu à l'écart.

Voici des exemples de planques :

- Une maison, appartement, ou autre espace loué en espèces avec une **fausse identité (p. 34)**.
- La maison d'une personne en qui tu as confiance et qui est d'accord de prendre le risque qu'implique cette complicité, mais qui est suffisamment éloignée des réseaux sous surveillance.

Si un adversaire découvre une cachette ou une planque, il pourrait se mettre à la surveiller pour t'identifier quand tu y accèdes, comme cela s'est produit en Italie où des caméras à détection de mouvement ont été installées pour surveiller une cachette dans une forêt[34]. À cause de ça, en accédant à une cachette ou planque, tu peux :

- Faire de l'**anti-surveillance (p. 5)** pour contrer le risque de surveillance physique.
- Porter une **tenue anonyme (p. 52)** pour contrer le risque d'être observé ou filmé.
- Prendre des **mesures de détection d'accès physique (p. 38)** pour t'assurer que la cachette ou la planque n'a pas été accédée physiquement par un adversaire.

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

- N'utilise pas de gants en cuir car ils peuvent laisser leurs propres empreintes uniques sur les surfaces que tu touches (appelées *glove prints*[48]).
- N'utilise pas de gants de travail seuls car ils sont généralement perméables, et peuvent laisser passer ta sueur (et donc ton ADN).

Et prends des précautions adaptées :

- Assure-toi que ton ADN n'est pas déjà présent à l'extérieur des gants, car il serait transféré des gants vers toute surface que tu touches. Pour t'en assurer, tu peux utiliser une paire de gants neuve dans son emballage hermétique.
- Ne laisse pas ton ADN à l'extérieur des gants quand tu les enfiles. Pour t'en assurer, tu dois les enfiler sans toucher l'extérieur des gants[49].
- Quand tu portes les gants, ne touche pas ta peau ni toute surface qui pourrait contenir ton ADN, car l'ADN serait transféré de la surface vers les gants, et de là vers toute surface que tu touches.

Tu peux porter plusieurs paires de gants les unes sur les autres. Par exemple, porter des gants de travail par-dessus des gants épais en latex ou caoutchouc garantit à la fois la robustesse des gants de travail et l'imperméabilité des gants épais en latex ou caoutchouc.

Si tu portes des gants pour éviter de laisser de l'ADN sur les surfaces que tu touches, tu voudras aussi éviter de laisser de l'ADN d'autres façons (par exemple des bouts de peau ou des poils qui tombent de ton corps). Pour plus d'informations, voir la mesure d'atténuation connexe **Protocoles de minimisation de l'ADN (p. 43)**.

[48]https://en.wikipedia.org/wiki/Glove_prints

[49]Pour faire ça, pince l'intérieur du gant gauche avec ta main droite et mets ta main gauche dedans (si tu es droitièr·e, sinon l'inverse), puis pince l'extérieur du gant droit avec ta main gauche gantée et mets ta main droite dedans.

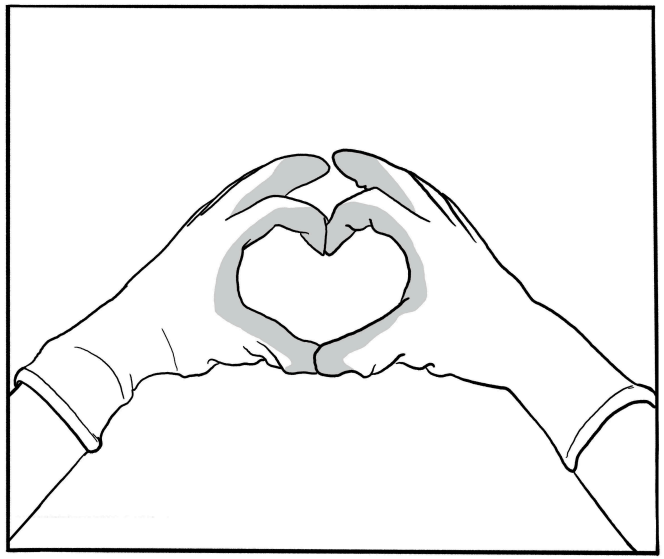
- Pour entrer en **clandestinité (p. 21)**.

5.19. Gants

Techniques contrées par cette mesure d'atténuation :

Science forensique > ADN (#3)

Science forensique > Empreintes digitales (#3)



Les gants peuvent t'empêcher de laisser des empreintes digitales et de l'ADN sur les surfaces que tu touches, et peuvent cacher les caractéristiques de tes mains.

Empreintes digitales et ADN

Pour éviter de laisser des empreintes digitales et de l'ADN sur les surfaces que tu touches, utilise le bon type de gants :

- Utilise des gants imperméables épais, en latex ou en caoutchouc.
- N'utilise pas de gants fins (comme des gants fins en latex ou caoutchouc) car tes empreintes peuvent passer à travers.

5.7. Chiffrement

Techniques contrées par cette mesure d'atténuation :

Collaboration des fournisseurs de service > Autres (#2)

Collaboration des fournisseurs de service > Opérateurs de téléphonie mobile (#2)

Science forensique > Numérique (#3)

Surveillance de masse > Surveillance numérique de masse (#3)

Surveillance numérique ciblée > IMSI-catcher (#3)

Surveillance numérique ciblée > Malware (#3)

Surveillance numérique ciblée > Science forensique appliquée aux réseaux informatiques (#3)

Le chiffrement est un processus qui rend des données inintelligibles par quiconque ne possède pas la clé de déchiffrement (souvent un mot de passe). Le chiffrement peut être appliqué à des données « au repos » (comme les fichiers stockés sur ton ordinateur) ou des données « en mouvement » (comme les messages d'une application de messagerie).

Tu peux chiffrer les données « au repos » d'un appareil numérique en activant le *chiffrement complet du disque* sur l'appareil avec un **mot de passe robuste (p. 9)**. Quand l'appareil est éteint, ses données sont chiffrées ; quand tu l'allumes et que tu entres la clé de déchiffrement, ses données sont déchiffrées jusqu'à ce qu'il soit éteint. Si un appareil avec chiffrement complet du disque est saisi par un adversaire pendant une arrestation, **perquisition (#2)** ou une **visite discrète de domicile (#3)** alors qu'il est éteint, l'adversaire ne pourra pas accéder à ses données (à moins qu'il ne **contourne son authentification (#3)**).

Tu peux chiffrer des données « en mouvement » en utilisant Tor[22] ou un Virtual Private Network (VPN) quand tu utilises Internet, et en utilisant des **applications de messagerie chiffrées de bout-en-bout (p. 9)** pour tes communications numériques. Chiffrer les données « en mouvement » peut empêcher un adversaire de surveiller tes activités numériques.

Le chiffrement devrait être considéré comme une mesure de réduction des risques, pas une panacée. Tu ne devrais pas utiliser d'appareils numériques pour des activités incriminantes sauf si tu ne peux pas faire autrement, et toutes tes conversations incriminantes devraient avoir lieu **en extérieur et sans appareils électroniques (p. 23)**.

5.8. Clandestinité

Techniques contrées par cette mesure d'atténuation :

Perquisition (#2)
Visite discrète de domicile (#3)

La clandestinité est le processus qui consiste à te séparer de ton identité actuelle et à démarrer une nouvelle vie sous une **fausse identité (p. 34)**.

Tu peux entrer en clandestinité :

- En réaction à la répression, par exemple pour éviter la prison, ou après t'être évadé·e de prison.
- Pour participer à une organisation clandestine, c'est-à-dire une organisation au sein de laquelle il a été décidé que tous les membres devraient entrer en clandestinité.

Voir le sujet « Clandestinité »[35].

5.9. Cloisonnement

Techniques contrées par cette mesure d'atténuation :

Cartographie de réseau (#2)
Surveillance numérique ciblée > Malware (#3)
Surveillance numérique ciblée > Science forensique appliquée aux réseaux informatiques (#3)

Le cloisonnement est un principe de sécurité selon lequel différentes identités (ou projets) sont séparées les unes des autres

[35]https://notrace.how/resources/fr/#topic=clandestinity

- Ne laisse rien d'incriminant passer par ton téléphone (messages, photos, etc.), même si tu utilises des applications de messagerie chiffrées de bout-en-bout.
- N'utilise pas de réseaux sociaux, ou au moins ne poste rien d'incriminant sur des réseaux sociaux. Les réseaux sociaux sont une mine d'informations pour des adversaires étatiques.
- Ne prends pas de photos ou vidéos pendant des émeutes. Prendre des photos ou vidéos pendant des émeutes incrimine des gens et devrait être considéré comme une forme de délation[47].

5.18. Fausse identité

Techniques contrées par cette mesure d'atténuation :

Cartographie de réseau (#2)
Vérifications d'identité (#3)

Une fausse identité est une identité que tu adoptes à la place de ton identité réelle pour éviter d'être détecté·e par un adversaire. Tu peux avoir plusieurs fausses identités, et tu peux alterner entre ton identité réelle et tes fausses identités en fonction du contexte.

Une fausse identité peut se composer de :

- Un faux nom, lieu et date de naissance, et autres informations biographiques.
- Un faux historique famillial, de fausses expériences professionnelles, et autres informations personnelles.
- De faux documents d'identité.

Tu peux utiliser une fausse identité :

- Pour contrer la **cartographie de réseau (#2)** ou éviter une arrestation en cas de **contrôle d'identité (#3)**.
- Pour mettre en place une **planque (p. 18)**.

[47]https://rosecitycounterinfo.noblogs.org/2022/08/uprising-lessons

Éviter l'auto-incrimination signifie ne pas donner des informations à un adversaire qui pourraient être utilisées pour t'incriminer, toi ou tes camarades. Un grand nombre de condamnations sont basées sur des informations obtenues par de l'auto-incrimination.

Ne parle pas à la police

Si tu es arrêté·e par un adversaire étatique, ne parle pas à la police. Toute communication pourrait être utilisée pour t'incriminer, toi ou tes camarades.

Les exceptions à cette règle incluent :

- Dans de nombreux contextes, tu peux être forcé·e de fournir à la police une forme d'identification (souvent ton nom, date et lieu de naissance) pour éviter d'être arrêté·e ou d'autres conséquences négatives.
- Dans certains contextes, tu peux être forcé·e de fournir à la police tes informations biométriques (photo de ton visage, empreintes digitales, ADN).

Voir Comment la police interroge et comment s'en défendre[46] sur comment se protéger des techniques d'interrogatoire de la police.

Principe du #emph[need-to-know]

Applique le **principe du** *need-to-know* **(p. 41)**. En particulier, ne te vante pas de tes crimes auprès d'amis, camarades, ou compagnon·ne·s de cellule—même si vous vous faites pleinement confiance, l'information met inutilement en danger la personne à qui tu la communiques et pourrait être entendue par un adversaire.

Bonnes pratiques numériques

Adopte de **bonnes pratiques numériques (p. 9)**. En particulier :

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

pour qu'elles ne puissent pas être reliées, et que si l'une d'elles est compromise, les autres ne le soient pas. Ce principe s'applique aussi bien à des identités numériques que non-numériques.

Voici des exemples de cloisonnement numérique :

- Utiliser différentes adresses email pour différentes identités numériques, par exemple une adresse professionnelle, une autre pour les ami·e·s, une autre pour un projet sensible particulier, etc. Ainsi, si un adversaire connaît ton adresse email professionnelle et découvre ton adresse email sensible après avoir saisi un ordinateur lors d'une perquisition, comme les adresses sont différentes il ne pourra pas relier l'adresse email sensible à ton identité.
- Utiliser différentes clés USB Tails[36] ou machines virtuelles Qubes OS[37] pour différentes identités numériques. Ainsi, si un adversaire compromet une clé ou une machine virtuelle avec un **malware (#3)**, les autres clés ou machines virtuelles ne seront pas compromises.

Voici des exemples de cloisonnement non-numérique :

- Utiliser différents noms dans différents contextes, par exemple ton nom civil avec ta famille et un pseudonyme avec tes ami·e·s. Un pseudonyme peut être spécifique à un endroit, moment, ou groupe de personnes avec lesquelles tu interagis. Ainsi, si un adversaire compromet l'un de tes noms, tes autres noms ne seront pas forcément compromis.
- Appliquer le **principe du** *need-to-know* **(p. 41)** en ne partageant des informations sensibles que lorsque c'est nécessaire, et dans la mesure du nécessaire.

Le cloisonnement peut aussi être un outil utile pour se souvenir d'appliquer des mesures d'atténuation de manière systématique au sein d'un projet. Par exemple, tu peux vouloir toujours prendre des mesures d'**anti-surveillance (p. 5)** lorsque tu voyages dans le

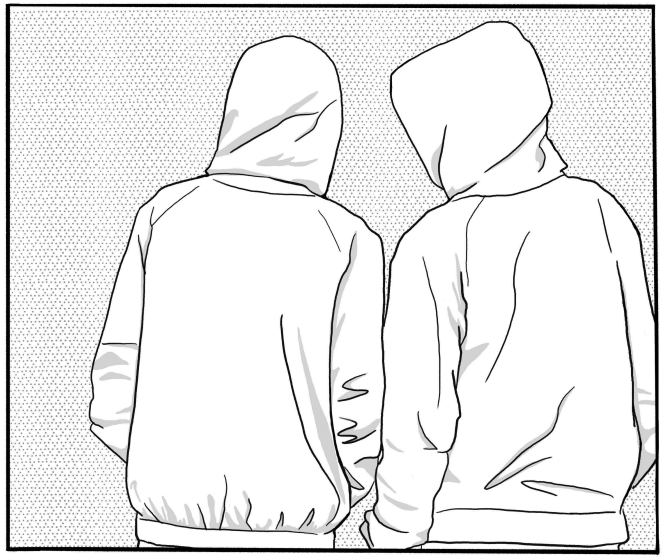
[36]https://tails.net
[37]https://www.qubes-os.org

cadre d'un projet donné, mais ne pas faire le même effort pour un autre projet moins sensible.

5.10. Conversations en extérieur et sans appareils

Techniques contrées par cette mesure d'atténuation :

Dispositifs de surveillance cachés > Audio (#2)
Surveillance de masse > Vidéosurveillance (#3)



Les conversations en extérieur et sans appareils sont la pratique qui consiste à avoir des conversations incriminantes en extérieur et sans appareils électroniques, pour s'assurer qu'elles ne puissent pas être écoutées par un adversaire.

Les conversations en extérieur et sans appareils sont nécessaires parce que :

- Les espaces intérieurs, y compris les voitures, peuvent contenir des **dispositifs de surveillance cachés (#2)**.

Pour les fichiers numériques, l'effacement des métadonnées peut être effectué avec MAT2[44] ou des logiciels similaires. Certains **systèmes d'exploitation axés sur la sécurité (p. 9)** intègrent par défaut des outils d'effacement des métadonnées.

Protection des métadonnées

Voici des exemples de protection des métadonnées :

- Utiliser un système d'exploitation dédié (par exemple une clé Tails[14]) pour créer ou modifier des fichiers numériques, pour que des informations relatives au système d'exploitation que tu utilises d'habitude ne se retrouvent pas dans les métadonnées des fichiers.
- Utiliser des **applications de messagerie qui protègent les métadonnées (p. 9)**.

Voir aussi

Voir le guide d'AnarSec « Remove Identifying Metadata From Files »[45] (*Supprime les métadonnées identifiantes de fichiers*) sur comment supprimer les métadonnées de fichiers numériques.

5.17. Éviter l'auto-incrimination

Techniques contrées par cette mesure d'atténuation :

Cartographie de réseau (#2)
Frapper aux portes (#2)
Open-source intelligence (#2)
Science forensique > Numérique (#3)
Surveillance de masse > Surveillance numérique de masse (#3)
Techniques d'interrogatoire (#3)
Vérifications d'identité (#3)

[44] https://github.com/tpet/mat2
[45] https://anarsec.guide/posts/metadata

Voir le sujet « Reconnaissance faciale »[42] et le chapitre « Traces » de Prisma[2].

5.16. Effacement et protection des métadonnées

Techniques contrées par cette mesure d'atténuation :

Science forensique > Numérique (#3)

Les métadonnées sont des données à propos de données, c'est-à-dire des informations à propos d'autres informations. L'effacement des métadonnées est la suppression des métadonnées. La protection des métadonnées est la capacité d'un système numérique à ne pas créer de métadonnées en premier lieu, ou à chiffrer les métadonnées qu'il crée de manière à ce qu'elles ne puissent pas être lues par un adversaire.

Exemples de métadonnées

Voici des exemples de métadonnées :

- Un fichier image peut contenir des informations sur quand est-ce que l'image a été prise et sur l'appareil photo ou le téléphone qui l'a prise.
- Un fichier PDF peut contenir des informations à propos de l'ordinateur qui l'a créé.
- Un email contient l'adresse email qui l'a envoyé et l'adresse email qui l'a reçu.
- Un document imprimé possède souvent un filigrane invisible[43] qui identifie la marque et le modèle de l'imprimante qui l'a imprimé.

Effacement des métadonnées

[42]https://notrace.how/resources/fr/#topic=facial-recognition
[43]https://eff.org/issues/printers

- Les apareils électroniques peuvent être infectés par des **malware (#3)** qui peuvent les transformer en microphones espions.

Les conversations en extérieur peuvent être enregistrées avec des microphones cachés ou des microphones paraboliques à longue portée lors d'une opération de **surveillance physique (#3)** (avec des portées jusqu'à 300 mètres). Par exemple, en Italie en 2019[38] un microphone était caché dans une fausse pierre devant une prison où des rassemblements avaient souvent lieu. Pour cette raison, tu devrais avoir tes conversations en extérieur en marchant, ou pour des conversations en grand groupe où il serait difficile de se déplacer, les avoir dans des endroits qui changent régulièrement et qui sont difficiles à placer sous surveillance audio.

Lors de conversations sans appareils, tu ne devrais pas éteindre ton téléphone, retirer sa batterie, ou le placer dans un sac de Faraday car cela génère des **métadonnées (p. 31)** à propos de qui a des conversations sensibles, quand, et où. Laisse plutôt ton téléphone chez toi. De plus, un sac de Faraday n'empêche pas l'audio d'être enregistré, seulement d'être transmis, ce qui pourrait se produire lors de la reconnexion du téléphone au réseau.

Voir le sujet « Culture de la sécurité »[39].

5.11. Déplacement en vélo

Techniques contrées par cette mesure d'atténuation :

Dispositifs de surveillance cachés > Localisation (#2)
Surveillance de masse > Vidéosurveillance (#3)
Surveillance physique > Cachée (#3)

Le déplacement en vélo est la pratique qui consiste à utiliser un vélo plutôt que d'autres moyens de transport.

Voici des avantages du déplacement en vélo :

[38]https://notrace.how/earsandeyes/fr/#cuneo-2019-06
[39]https://notrace.how/resources/fr/#topic=security-culture

- Les vélos sont plus difficiles que les voitures à identifier par la **vidéosurveillance (#3)** : la marque et le modèle d'un vélo peuvent être dissimulés et les vélos n'ont généralement pas de plaques d'immatriculation.
- Il est plus difficile pour une opération de **surveillance physique (#3)** de suivre un vélo qu'une voiture ou une personne à pied, surtout sans être détectée, et il est plus facile de faire de la **détection de surveillance (p. 27)** et de l'**anti-surveillance (p. 5)** depuis un vélo. Par exemple, pendant une opération de surveillance physique de six mois contre un anarchiste en France, la police a régulièrement perdu sa trace quand il faisait du vélo[40].
- Il y a beaucoup moins d'emplacements possibles pour installer un **dispositif de surveillance par localisation (#2)** sur un vélo que sur une voiture, et quand on **cherche (p. 44)** un vélo, on peut déterminer avec un haut degré de certitude si un dispositif de surveillance est présent ou non.

5.12. Dessiner une carte de son réseau

Techniques contrées par cette mesure d'atténuation :

Cartographie de réseau (#2)
Indics (#2)
Infiltré·e·s (#2)
Surveillance numérique ciblée > Accès physique (#3)

Dessiner une carte de ton réseau consiste à créer une représentation graphique des liens entre toi et les personnes de ton réseau afin d'examiner ces liens de manière critique. Cet exercice est conçu pour affûter ta capacité à faire des choix éclairés et critiques à propos des personnes avec qui tu t'associes, dans le but final de rendre ton réseau plus résistant aux tentatives d'**infiltration (#2)**.

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

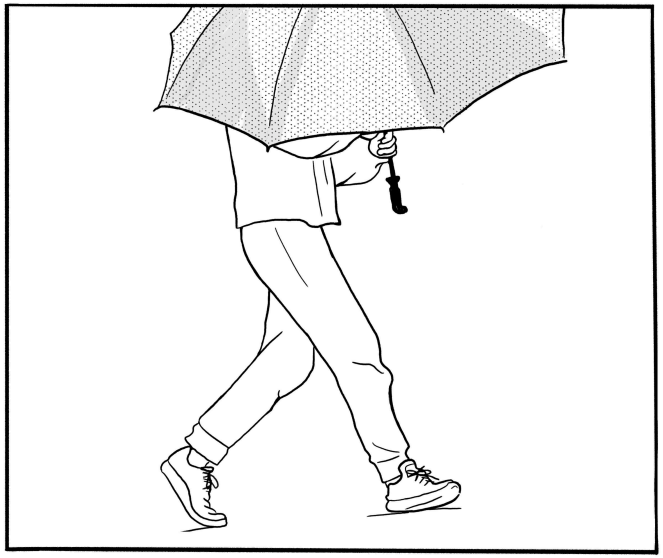
Voir aussi

- Surveillance Countermeasures[6] (*Mesures contre la surveillance*) à propos des principes et techniques de détection de surveillance.
- Le sujet « Surveillance physique »[7].
- La mesure d'atténuation connexe **Anti-surveillance (p. 5)**.

5.15. Dissimulation biométrique

Techniques contrées par cette mesure d'atténuation :

Science forensique > Analyse de l'écriture (#3)
Science forensique > Linguistique (#3)
Science forensique > Reconnaissance de démarche (#3)
Science forensique > Reconnaissance faciale (#3)
Surveillance de masse > Vidéosurveillance (#3)



La dissimulation biométrique inclue toute pratique consistant à cacher des identifiants biométriques (des caractéristiques physiques ou biologiques uniques) pouvant être utilisés dans un but d'identification.

du point de vue d'une potentielle opération de surveillance, mais cela devrait être illogique pour toute autre personne de le suivre, et il devrait inclure plusieurs arrêts permettant au tiers de tenter de détecter une opération de surveillance. Par exemple, tu peux commencer chez toi, t'arrêter à trois ou quatre magasins de bricolage dans ta ville en prétendant te renseigner sur le prix d'un objet, puis retourner chez toi. Cet itinéraire semblerait logique à une potentielle opération de surveillance, mais il est peu probable que qui que ce soit suive le même itinéraire, en s'arrêtant aux mêmes magasins dans le même ordre que toi.

2. Alors que tu suis l'itinéraire choisi, le tiers s'assure qu'il est présent à chaque arrêt avant toi, mais sans prendre le même chemin que toi (pour éviter d'être détecté par une potentielle opération de surveillance). Pour ça, le tiers peut utiliser un moyen de transport plus rapide que toi, ou partir de chaque arrêt avant toi pour prendre de l'avance, ou utiliser plusieurs équipes coordonnées.
3. À chaque arrêt, le tiers prend note des piétons et véhicules qui arrivent après toi. Si le tiers remarque qu'un piéton ou véhicule est présent à deux arrêts ou plus, il est peut-être un opérateur de surveillance. Le tiers peut aussi détecter des comportements typiques d'opérateurs de surveillance, comme le fait de transmettre des informations via une radio cachée sur eux, le fait de communiquer entre eux par signes visuels, de se mettre à courir de manière inattendue, etc.

Considérations supplémentaires

Si un adversaire remarque que tu fais de la détection de surveillance, il pourrait s'adapter et se faire plus discret. Quand tu fais de la détection de surveillance, tu devrais donc éviter de révéler que tu le fais, si possible. Si tu détectes avec succès une opération surveillance, tu devrais éviter de le faire savoir de manière visible ou d'échapper à l'opération de surveillance.

Une idée centrale de cet exercice est de t'aider à réfléchir pas seulement au niveau de tes groupes affinitaires, mais à un niveau plus global qui inclut des personnes que tu ne connais pas bien, et peut même inclure des personnes que tu ne connais vraiment pas. L'exercice consiste à se poser une série de questions structurées qui révèlent ton niveau de sécurité avec chaque personne de ton réseau, à partir de quoi tu dessines une carte qui distingue les personnes en qui tu fais confiance des personnes que tu aimerais apprendre à mieux connaître. L'exercice est plutôt conçu pour être fait dans des périodes calmes.

Pour des instructions sur comment faire ça, voir Arrêtons de chasser les moutons : Un guide pour créer des réseaux plus sûrs[41]. Une telle carte de ton réseau serait inestimable pour un adversaire—c'est à peu près ce qu'il construit avec la **cartographie de réseau (#2)**—et devrait donc être brûlée immédiatement après utilisation.

5.13. Détection d'intrusion physique

Techniques contrées par cette mesure d'atténuation :

Dispositifs de surveillance cachés > Audio (#2)
Dispositifs de surveillance cachés > Localisation (#2)
Dispositifs de surveillance cachés > Vidéo (#2)
Fabrication de preuves (#2)
Surveillance numérique ciblée > Accès physique (#3)
Visite discrète de domicile (#3)

La détection d'intrusion physique est le processus qui consiste à détecter quand un adversaire entre ou tente d'entrer dans un espace, par exemple dans le cadre d'une **visite discrète de domicile (#3)**. Tu peux accomplir cela en faisant en sorte qu'il y ait toujours une personne dans l'espace qui remarquerait si un adversaire essayait d'entrer, ou en surveillant l'espace à l'aide d'un système de vidéosurveillance.

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

Un système de vidéosurveillance qui surveille un espace peut avoir les caractéristiques suivantes :

- Les caméras peuvent détecter les mouvements et t'envoyer une alerte si elles sont détectées et trafiquées.
- Les caméras peuvent être positionnées avec les entrées de l'espace dans leur ligne de vue et/ou dans un endroit discret.
- Pour empêcher le système de te surveiller toi quand tu es dans l'espace, tu peux l'allumer juste avant de quitter l'espace et l'éteindre dès que tu reviens.

5.14. Détection de surveillance

Techniques contrées par cette mesure d'atténuation :
Dispositifs de surveillance cachés > Vidéo (#2)
Surveillance physique > Aérienne (#3)
Surveillance physique > Cachée (#3)

La détection de surveillance est la pratique qui consiste à détecter si tu es sous **surveillance physique (#3)**, c'est-à-dire, détecter si tu es en train d'être directement observé·e par un adversaire. Il y a deux types de détection de surveillance : la détection passive de surveillance et la détection active de surveillance. La contre-surveillance est une forme sophistiquée de détection active de surveillance.

Détection passive de surveillance

La détection passive de surveillance c'est quand tu détectes la surveillance sans dévier de ta routine habituelle. Voici des exemples de détection passive de surveillance :

- Vérifier régulièrement les rétroviseurs dans un véhicule en mouvement pour détecter des véhicules de surveillance en train de te suivre.
- Écouter les bruits ambiants pour détecter des drones ou hélicoptères en train de voler au-dessus de toi.

Détection active de surveillance

La détection active de surveillance c'est quand tu détectes la surveillance en agissant en-dehors de ta routine habituelle pour tenter de forcer une potentielle opération de surveillance à se dévoiler. Voici des exemples de détection active de surveillance :

- Suivre un itinéraire illogique pour se déplacer entre deux points, par exemple un itinéraire qui n'est pas le plus court. Si un piéton ou véhicule suit le même itinéraire illogique que toi, il est peut-être un opérateur de surveillance. Si possible, tu devrais avoir une raison valide de suivre cet itinéraire illogique (par exemple t'arrêter à un magasin sur l'itinéraire), pour qu'une opération de surveillance ne remarque pas que tu fais de la détection de surveillance.
- Faire un demi-tour inattendu en conduisant. Si tu es suivi·e par une équipe de surveillance incompétente (ou un seul véhicule de surveillance), un véhicule de surveillance pourrait reproduire ton demi-tour, ce qui serait un signe clair qu'il te suit. Si tu es suivi·e par une équipe de surveillance compétente qui dispose de plusieurs véhicules, les véhicules de surveillance ne vont pas reproduire ton demi-tour, car cela serait suspect, mais ton demi-tour peut tout de même provoquer chez eux des réactions anormales, ce qui peut t'aider à les détecter. Si possible, tu devrais avoir une raison valide de faire le demi-tour, pour qu'une opération de surveillance ne remarque pas que tu fais de la détection de surveillance.

Contre-surveillance

La contre-surveillance c'est quand tu détectes la surveillance avec l'aide d'un tiers de confiance (c'est-à-dire une ou plusieurs personnes) qui n'est a priori pas sous surveillance, et qui tente de détecter si tu es sous surveillance. Voici un exemple d'une opération de contre-surveillance :

1. Choisis l'itinéraire que tu vas prendre pendant l'opération de contre-surveillance. L'itinéraire devrait sembler logique