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

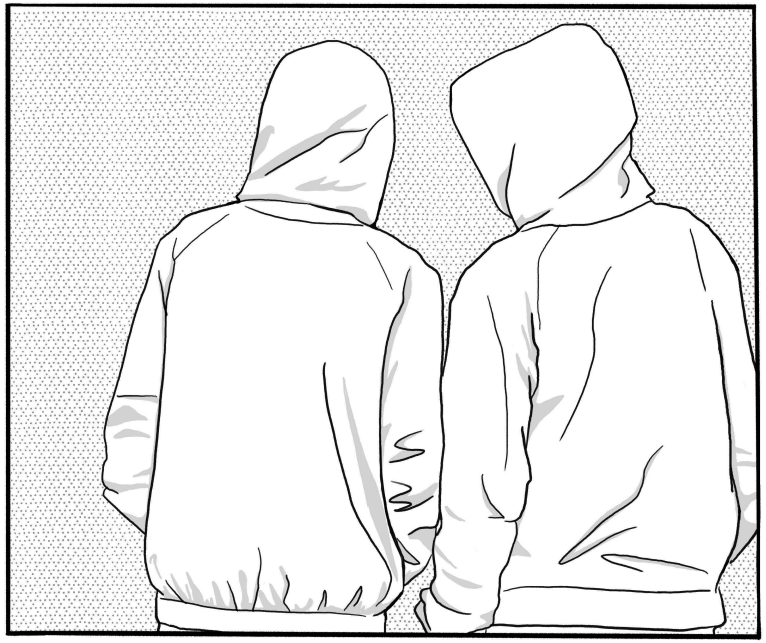
No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

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

# Bibliothèque de menaces

## Partie 1/5

## Tutoriel, Tactiques



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

**Texte d'origine en français**

No Trace Project

notrace.how/threat-library/fr

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

7 juin 2025

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

**Open-source intelligence (#2)**
**Patrouilles de police (#2)**
**Perquisition (#2)**
**Science forensique (#3)**
**Surveillance de masse (#3)**
**Surveillance numérique ciblée (#3)**
**Surveillance physique (#3)**
**Techniques d'interrogatoire (#3)**
**Violence physique (#3)**
**Visite discrète de domicile (#3)**
**Vérifications d'identité (#3)**

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

## 3.3. Arrestation

Utilise les techniques :

**Augmentation de la présence policière (#2)**
**Chiens de détection (#2)**
**Coopération internationale (#2)**
**Patrouilles de police (#2)**
**Perquisition (#2)**
**Systèmes d'alarme (#3)**
**Vigiles (#3)**
**Vérifications d'identité (#3)**

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

# 3. Tactiques

## 3.1. Dissuasion

Utilise les techniques :

**Augmentation de la présence policière (#2)**
**Doxing (#2)**
**Frapper aux portes (#2)**
**Patrouilles de police (#2)**
**Surveillance de masse (#3)**
**Violence physique (#3)**

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

## 3.2. Incrimination

Utilise les techniques :

**Cartographie de réseau (#2)**
**Chiens de détection (#2)**
**Collaboration des fournisseurs de service (#2)**
**Construction parallèle (#2)**
**Coopération internationale (#2)**
**Dispositifs de surveillance cachés (#2)**
**Fabrication de preuves (#2)**
**Frapper aux portes (#2)**
**Indics (#2)**
**Infiltré·e·s (#2)**
**Interprétation biaisée des preuves (#2)**



# Sommaire


**1. À propos de la Bibliothèque de menaces . . . . . 3**
1.
1.1. Modélisation de menaces . . . . . 3
1.2. La Bibliothèque de menaces . . . . . 4
1.3. Limites . . . . . 5

**2. Tutoriel : utilisation de la Bibliothèque de menaces avec des arbres d'attaque . . . . . 6**
2.
2.1. Un exemple simple : sécher un jour d'école . . . . . 7
2.2. Un vrai exemple : une émeute dans une grande ville des États-Unis . . . . . 9
2.2.1. Dessiner l'arbre d'attaque . . . . . 9
2.2.2. Identifier les techniques . . . . . 15
2.2.3. Identifier les mesures d'atténuation . . . . . 17
2.2.4. Décider comment implémenter les mesures d'atténuation . . . . . 18
2.2.5. Brûler ou numériser vos notes . . . . . 20
2.2.6. Débriefing de l'action . . . . . 21
2.3. Évaluer les risques . . . . . 21
2.3.1. Impact . . . . . 22
2.3.2. Probabilité . . . . . 22
2.3.3. Les ressources de l'adversaire augmentent le risque . 22
2.3.4. Les mesures d'atténuation réduisent le risque . . . . . 23
2.3.5. Risque et contexte local . . . . . 23
2.4. Conseils supplémentaires pour utiliser la Bibliothèque de menaces . . . . . 24

**3. Tactiques . . . . . 25**
3.
3.1. Dissuasion . . . . . 25
3.2. Incrimination . . . . . 25
3.3. Arrestation . . . . . 26

# 1. À propos de la Bibliothèque de menaces

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

## 1.1. Modélisation de menaces

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

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

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



## 2.4. Conseils supplémentaires pour utiliser la Bibliothèque de menaces

La matrice[9] de la Bibliothèque de menaces présente une vue d'ensemble de toutes les tactiques et techniques, ainsi que des boutons qui te permettent de cacher ou d'afficher des techniques spécifiques. Par exemple, tu peux vouloir afficher seulement les techniques qui correspondent à ton modèle de menace pour mieux les visualiser. Si tu suis le processus que nous proposons ci-dessus et que tu dessines ton propre arbre d'attaque, la vue d'ensemble peut t'aider à penser à des techniques pertinentes qui manquent à ton arbre.

La Bibliothèque de menaces accepte les contributions externes, comme :

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

Voir la **section « Contribuer » (#5)** pour plus d'informations.

plus probable que la scène de crime soit fouillée en profondeur pour y trouver des preuves ADN.

- Dans la plupart des contextes, si l'adversaire est l'État, des actions classifiées comme « terrorisme » ou « menaces à la sécurité nationale » vont recevoir des quantités extraordinaires de ressources. L'État peut dévouer beaucoup de ressources à des actions qui ont eu lieu pendant un soulèvement, parce que le soulèvement a été perçu comme une menace à son intégrité.

### 2.3.4. Les mesures d'atténuation réduisent le risque

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

Par exemple, tu es vulnérable aux analyses ADN parce que de l'ADN tombe en continu de ton corps. Si tu appliques des **protocoles de minimisation de l'ADN (#4)** en commettant un incendie volontaire, tu deviens moins vulnérable aux analyses ADN.

### 2.3.5. Risque et contexte local

Comprendre les habitudes et motivations d'un adversaire dans la répression d'une action peut t'aider à identifier le panel de techniques répressives qu'il utilisera probablement, et avec quelle minutie il les utilisera. Les **opérations répressives (#5)** peuvent t'aider à comprendre comment une technique donnée est utilisée dans un contexte donné.

[9] https://notrace.how/threat-library/fr/matrix.html



## 1.2. La Bibliothèque de menaces

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

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

La Bibliothèque de menaces contient de nombreuses informations sur les techniques répressives d'État. Cela peut avoir un effet paralysant, en faisant paraître l'État comme tout-puissant. L'État n'est pas tout-puissant.[2] L'intention de la Bibliothèque de menaces n'est ni de minimiser ni d'exagérer les capacités de l'État, mais plutôt de

[2] En réalité, la grande majorité des actions directes anarchistes ne sont pas poursuivies en justice. Des enquêteurs frustrés de Bremen, en Allemagne[3] et de Grenoble, en France[4] ont lamenté dans les médias leur incapacité à réprimer un seul des incendies volontaires qui ont eu lieu dans les deux villes au fil des

comprendre les options à sa disposition et comment ces options sont utilisées dans différents contextes.

## 1.3. Limites

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

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

---

années, phénomène qu'ils attribuent aux mesures d'atténuation prises par les incendiaires.

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

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



### 2.3.1. Impact

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

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

### 2.3.2. Probabilité

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

### 2.3.3. Les ressources de l'adversaire augmentent le risque

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

Par exemple :

- Dans la plupart des contextes, des analyses ADN sont systématiquement réalisées dans les enquêtes sur des incendies volontaires. Si l'adversaire a des ressources limitées, les prélèvements peuvent être limités à des surfaces évidentes comme des poignées de porte. Si l'adversaire a plus de ressources—ce qui peut être le cas si l'incendie a causé beaucoup de dégâts—il est

pas d'adopter de **bonnes pratiques numériques (#4)**). Tu peux utiliser Libreoffice Draw (inclus dans Tails par défaut) pour dessiner l'arbre d'attaque. Une fois les notes numérisées, elles ne devraient pas être imprimées parce que cela pourrait laisser des traces sur l'imprimante, mais elles peuvent être de nouveau copiées manuellement sur papier pour pouvoir les relire loin des écrans.

### *2.2.6. Débriefing de l'action*

Après l'émeute, toi et tes camarades prenez du temps pour faire un débriefing de l'action : dans des **conversations en extérieur et sans appareils (#4)**, vous discutez de ce qui s'est bien ou mal passé, et de si vous pouvez améliorer votre arbre d'attaque ou la manière dont vous avez implémenté les mesures d'atténuation.

## 2.3. Évaluer les risques

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

Par exemple, dans la plupart des contextes, si tu prévois de commettre un incendie volontaire, la technique **Science forensique : ADN (#3)** est très risquée. En effet, elle a un fort impact (une correspondance ADN avec la scène de crime d'un incendie volontaire est une preuve solide dans un procès) et une forte probabilité (dans la plupart des contextes, des analyses ADN sont systématiquement réalisées dans les enquêtes sur des incendies volontaires).



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

La Bibliothèque de menaces contient beaucoup d'informations. Ça peut être un peu écrasant. Comment est-ce que tu peux utiliser la Bibliothèque de menaces dans ta vie, dans un projet particulier, ou quand tu fais des actions ? Ce tutoriel est conçu pour t'aider à utiliser la Bibliothèque de menaces avec des *arbres d'attaque*.[5]

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

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

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

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

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

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

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



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

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

### 2.2.5. Brûler ou numériser vos notes

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

1. À la fin de l'exercice, tu mémorises les notes et tu les brûles. Avec cette approche, c'est difficile de reprendre les notes plus tard pour les retravailler.
2. À la fin de l'exercice, tu numérises les notes en les retapant manuellement sur une clé USB chiffrée avec Tails[8] (n'oublie

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

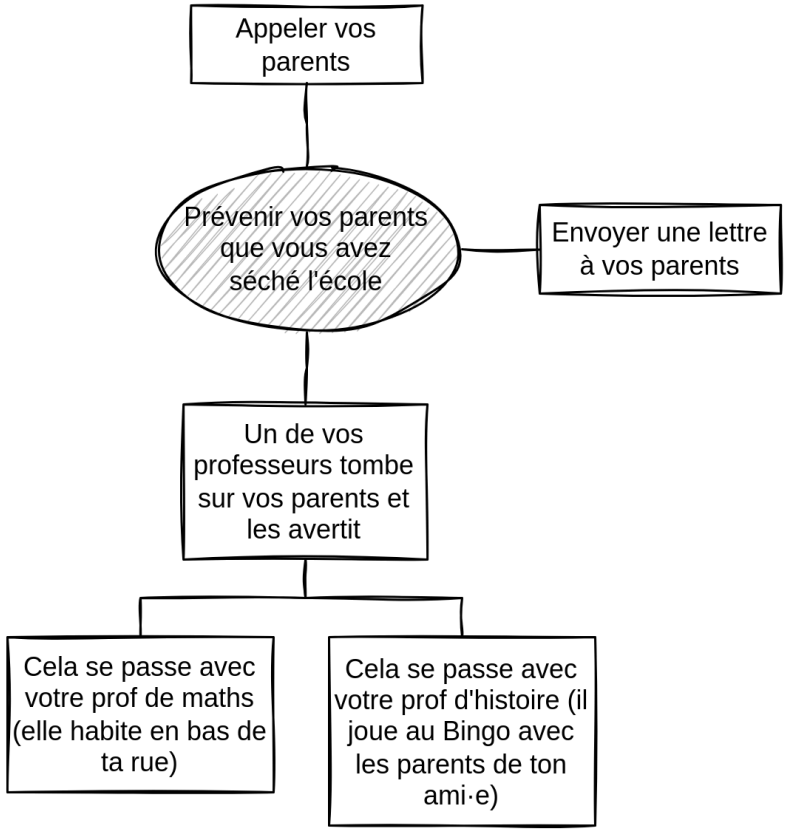
que d'autres camarades sachent comment vous soutenir si cela se produit.

- « Se préparer aux perquisitions » : Vous décidez d'arrêter de stocker les feux d'artifices sous ton lit.
- « Cachette ou planque » : Vous décidez d'enterrer un contenant hermétique dans une forêt proche pour stocker les feux d'artifice. Quand l'un·e d'entre vous y accède, iel doit porter des gants et s'assurer qu'il n'y a personne à proximité.
- « Bonnes pratiques numériques » : Vos appareils sont déjà chiffrés, et de toute façon vous ne les utilisez pas pour parler des émeutes. Vous devez vous renseigner pour savoir si le chiffrement d'un téléphone fonctionne quand il est allumé et verrouillé parce que vous n'êtes pas sûr·e·s.

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

Vous mettez à jour le tableau (8).






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

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

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

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

Disons que toi et quelques camarades vous vous préparez pour une émeute dans une grande ville des États-Unis. Vous voulez faire des dégâts, mais vous ne voulez pas vous faire prendre… Tu te tournes vers la Bibliothèque de menaces. Tu imprimes cette brochure, tu prends du papier et un crayon, et tu retrouves tes camarades **en extérieur et sans appareils électroniques (#4)**.

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

### 2.2.1. Dessiner l'arbre d'attaque

Dans cet exemple, l'adversaire est l'État et la police, et son but est d'obtenir suffisamment de preuves de votre participation à l'émeute pour convaincre un juge de vous condamner. Vous dessinez un arbre d'attaque pour répresenter comment il pourrait atteindre cet objectif.[7] Vous commencez avec le nœud racine (2).

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



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

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

### 2.2.4. Décider comment implémenter les mesures d'atténuation

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

- « Se préparer à la répression » : Comme toi et tes camarades vivez tou·te·s au même endroit, il y a un risque que vous soyez tou·te·s arrêté·e·s après une perquisition. Vous allez vous assurer

### 2.2.3. Identifier les mesures d'atténuation

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

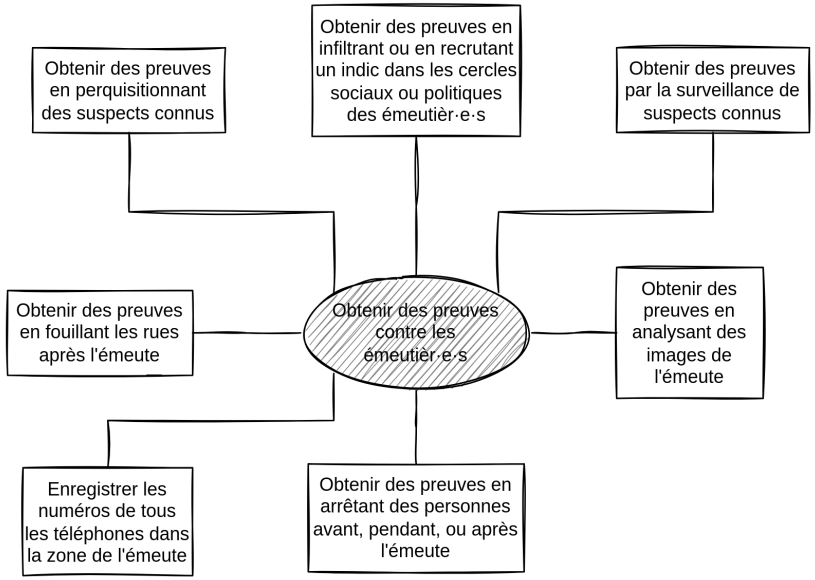
Pour la branche choisie pour cet exemple (5), vous décidez d'implémenter :

- Pour « Perquisition », **Se préparer à la répression (#4)**, **Se préparer aux perquisitions (#4)** et **Cachette ou planque (#4)**. Vous ne voulez pas implémenter **Clandestinité (#4)** parce que vous ne voulez pas entrer en clandestinité.
- Pour les deux techniques « Surveillance numérique ciblée », **Bonnes pratiques numériques (#4)** est la seule mesure d'atténuation qui a du sens dans votre contexte.

Vous mettez à jour le tableau (7).

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

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




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

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



- Les autres nœuds ne correspondent à rien, ils font juste partie de la perquisition.

À ce stade, ça peut être utile d'évaluer les risques des techniques que vous listez—ça vous aidera à décider quelles techniques vous voulez atténuer, et comment. Voir la section « Évaluer les risques », p. 21 sur comment évaluer les risques d'une technique en utilisant les concepts de *probabilité* et d'*impact*.

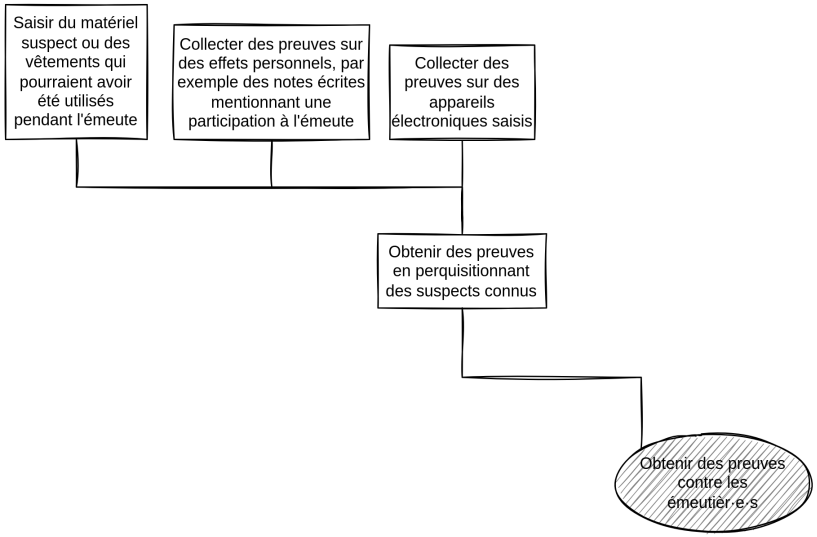
Ensuite vous passez à la branche suivante jusqu'à ce que tout l'arbre soit fait, en construisant un tableau (6).

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

(6) Début du tableau.

### 2.2.2. Identifier les techniques

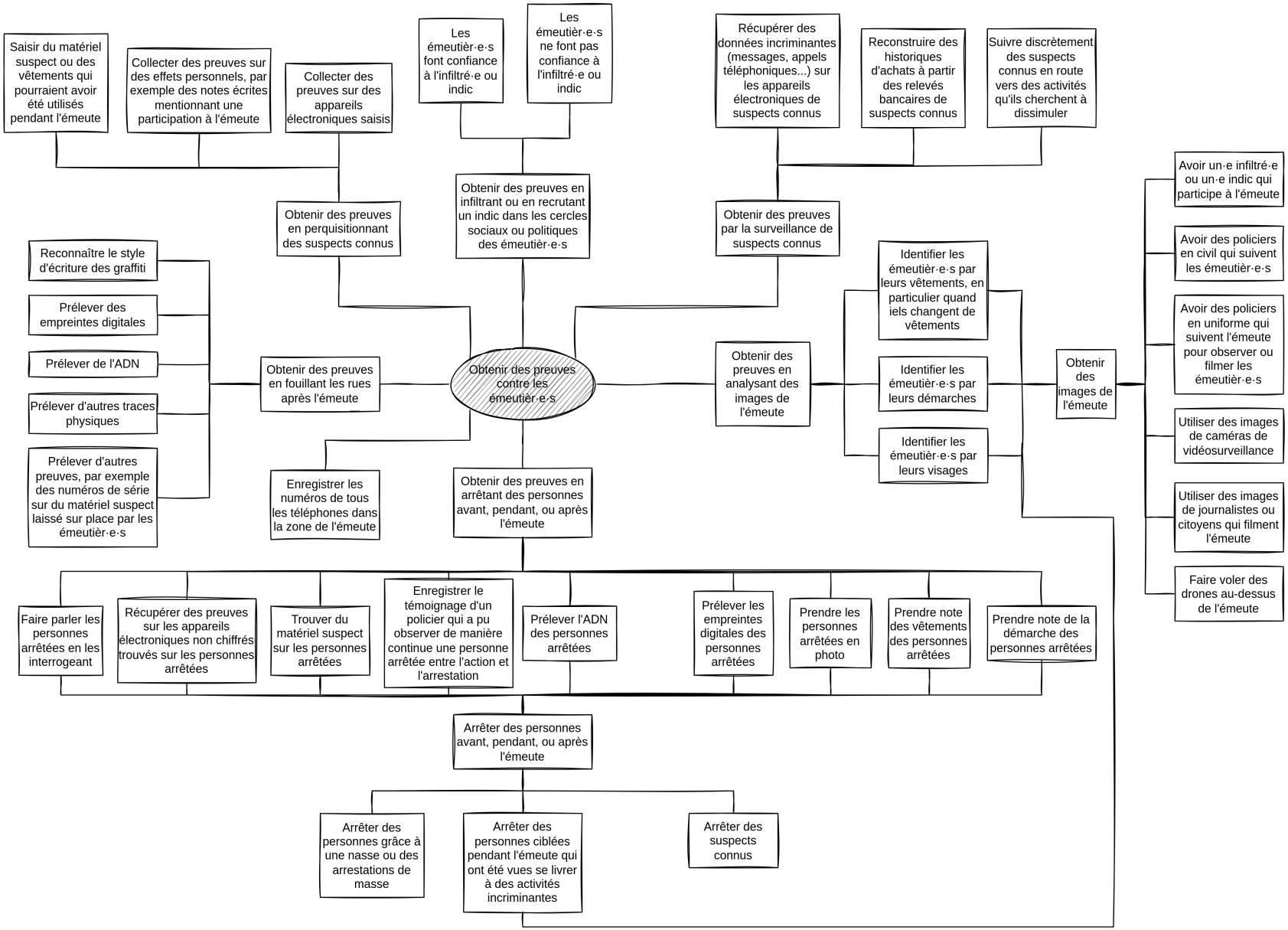
Vous identifiez toutes les techniques représentées sur l'arbre en associant les nœuds aux techniques de la Bibliothèque de menaces. Vous faites ça branche par branche pour éviter de vous perdre : c'est mieux de commencer par les nœuds les plus proches du nœud racine, puis de remonter la branche.




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

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

- « Obtenir des preuves en perquisitionnant des suspects connus » correspond à **Perquisition (#2)**.
- « Collecter des preuves sur des appareils électroniques saisis » correspond à **Surveillance numérique ciblée : Accès physique (#3)** parce qu'ils auraient besoin d'accéder à vos appareils électroniques, et à **Surveillance numérique ciblée : Contournement de l'authentification (#3)** si ils essaient de deviner vos mots de passe ou de casser le chiffrement.




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

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