Sécurité militante pour la coordination d'action

La **culture de sécurité** dépend du contexte mais elle se pense autours de la défense contre la **répression** (agir contre nous) et la **surveillance** (travail en amont pour savoir comment nous fonctionnons).

Dans le cas d'une coordination d'action, il y a **quatre grands moments** à considérer :

1. La coordination de l'action
2. Le briefing
3. L'action
4. Le post-action

Sur deux axes principaux :

- **Risques**
- **Bonnes pratiques**

Lors de la coordination d'action

Risques

Deux grands risques sont à prendre en compte, que les FDO sachent :

- **qui fait partie de la coordination.**
- **connaîssent la cible et le mode d'action.**

Il n'y a peu de procès envers les coordinations d'action.

Bonnes Pratiques

- **Communication limitée :** Évoquez le moins possible de parler de l'action avec proches (vos amis ou partenaires). Chaque membre de la coordination doit se poser la question : « Est-ce que j'ai le droit ET le besoin de connaître/partager cette information ? ».
- **Échanges sécurisés :** Utilisez des moyens de communication sécurisées.
  - **Mattermost :** Ce n'est pas chiffré. Préférez des outils sécurisés comme signal.

    - **Signal :** Activez les messages éphémères par défaut et désactivez les notifications affichant le contenu sur le téléphone dévérouillé.
    - Cliquez pour consulter le tuto pour protéger votre communication sur internet
- **Évitez de borner avec le reste de la coordination :** Surtout durant les réunions, en vous mettant en mode avion ou en éteignant vos portables en amont des réunions.
- **Évitez paiement par CB :** Si vous faite une réunion de coordo physique quelque par, comme un bar, ne pas utiliser votre carte bleu, pour ne pas laisser de trace de votre rencontre
- **Lieux de stockage/réunions/Brief :** Évitez les lieux connus comme militants, car ils peuvent être sur écoute.
- **Discrétion lors des repérages :** Fondez-vous dans la masse et éviter d'envoyer des personnes connues des FDO.
- **Ayez des mots de passe robuste:** Utilisez une phrase longue et mémorisable et au moins 12 charactères sur votre téléphone, drive, ordinateur.
    - Vous pouvez utiliser pour cela des coffres forts de mot de passe comme **keepass** ou **Bitwarden**
- **Recrutement**: Lors du recrutement, faites attention aux informations partagées qui peuvent donner beaucoup d'indices sur la cible et la méthode d'action. Pour les rôles très spécifiques (grimpe, etc), il est préférable de le faire en cooptation car ils donnent en eux-mêmes beaucoup d'information.

Outils numériques et tutos

- Pour protéger votre activité en ligne (exemple: sites militants consultés) de la surveillance étatique, voici ce tutoriel
- Si vous avez des données militantes sur votre ordinateur, et qu'il n'a pas été nettoyé, voici ce tutoriel pour nettoyer les traces d'activité militante
- Si vous avez besoin d'effectuer une activité militante sur votre ordinateur au délà des sites et drives en ligne, voici ce tuto pour chiffrer vos données efficacement, et ce tuto pour utiliser Tails (ou une autre type clé USB bootable)

Lors du briefing d'action

Risques

- **Divulger des informations qui permettent d'empêcher l'action**
- **Faciliter les poursuites ou le fichage militant.**

Bonnes Pratiques

- **En ligne ou en personne ?** Si en personne, assurez-vous qu'il n'y ait pas de prises de photos ou de vidéos.

- **Contenu du brief :** Expurger le brief des éléments non nécessaires et qui donnent des indications sur la cible (exemple : dire "il ne faudra pas fumer" indique que c'est un endroit avec des risques d'incendie (aéroport, raffinerie), mieux vaut le dire sur place. Une bonne astuce est de faire le brief public a une personne de confiance en amont et de lui demander de deviner la cible et la méthode d'action.
- **Vérification des participants :** Vérifiez que les personnes sont bien qui elles prétendent par des connaissances mutuelles.
- **Attribution des rôles**: Soyez discrets sur les rôles et leurs attributions.
- **Attention ce que vous laissez visibles lors du brief**Ne laissez pas traîner des documents contenant des rôles, des pseudos, des informations sur la cible (carte, communiqué de presse, artivisme (banderole)).

Lors de l'action

Risques

- **Arrestation de masse**
- **Arrestation ciblée :** Prendre en compte que les personnes visibles ou connues ont plus de chances d'être arrêtées.

Bonnes Pratiques

- **Déploiement efficace :** Soyer rapide et éviter l'inertie de groupe en nommant des responsables de groupe/déploiement.
- **Arrestation de masse :** Planifiez la défense collective.
- **Réploiement efficace :** Planifiez la fin de l'action.

Post-action

Risques

- **Perquisitions et procès :** Conséquences mentales et économiques, que cela se produise immédiatement ou un an plus tard.

Bonnes Pratiques

- **Précautions** : Soyez attentif à ce qui se trouve dans votre appartement pour éviter des problèmes lors des perquisitions (ex. : téléphone, vêtements).
- **Détruisez les documents les plus sensibles**: Attribution des rôles.
- **Se faire rembourser indirectement** Il est préférable qu'une seule personne soit remboursée pour éviter que toute la coordination soit connue (en discuter avec le GST Finance).

Révision #8
Créé 7 décembre 2025 19:47:32 par olipop
Mis à jour 21 décembre 2025 17:59:52 par mollusque