Est ce que ça sert à quelque chose de mettre son portable dans un four micro-ondes ?

Bernardettes

Qui êtes vous ?

Présenter vous comme vous le souhaitez +

Votre niveau en sécurité numérique :
- Déjà participer à une formation ?
- Ingénieur.e en informatique ?
- Jamais touché à un ordinateur ?

N’hésitez pas à prendre des notes
à me demander les diapos

INTRODUCTION :

les objectifs de la formation

Conseil : N’utilisez jamais d’outils numériques !

CECI EST UNE FORMATION QUI NE VOUS SERVIRA PAS

Vous donner des bases de sécurité numérique anti-répression (savoir se défendre face à l’état)

Introduction – travail de groupe

Votre connaissance en culture de la sécurité numérique influe sur votre sécurité en tant que militant·e mais aussi sur la sécurité du groupe

Qui a déjà mis son portable dans un micro-onde pour une réunion ?

ÉCOUTE

Comment la police peut vous écouter ?

Quoi mettre en place contre ça ?

A quel point c’est probable ?

BORNAGE

Comment la police peut savoir que vous êtes où non à une réunion ?

Comment fonctionne le GPS, les antennes téléphoniques… ?

Écoutes

Comment est ce que la police peut vous écouter lors d’une réunion ?

Comment est ce que la police peut vous écouter lors d’une réunion ?

Lieu sonoriser (sur écoute)

Quelqu’un présent dans la réunion

Piratage d’un téléphone portable

Comment est ce que la police peut vous écouter lors d’une réunion ?

Lieu sonoriser (sur écoute)

Quelqu’un présent dans la réunion

Piratage d’un téléphone portable

Lieu sonorisé

Logement

Squat

Lieu militant

Voitures

Lieu de rassemblement récurrent

Le site « Ears and Eyes » a recensé 65 micros dans les 20 dernières années dans le milieu militant de gauche (3 en France, 45 en Italie)

Mais il y en bien plus car certains n’ont pas été trouvé et certains ne sont pas recensé (affaire du 8 décembre)

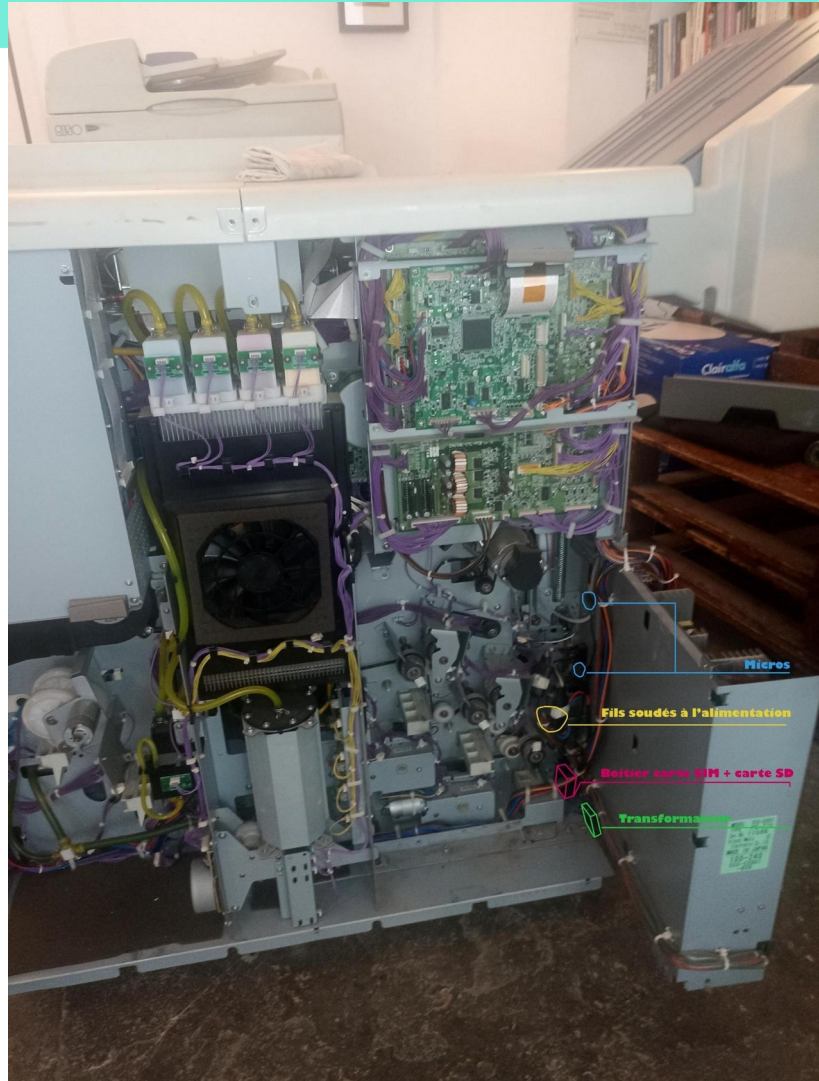
https://www.notrace.how/earsandeyes/fr/

Lieu sonorisé

Un microphone a été trouvé à la bibliothèque anarchiste Libertad à Paris

A l'intérieur de l'**imprimante-photocopieuse** de la bibliothèque.

Avril 2022



https://bibliothequelibertad.noblogs.org/post/2022/04/02/un-micro-trouve-a-la-bibliotheque-anarchiste-libertad/

Lieu sonorisé

Un microphone a été trouvé au squat Awhanee à Grenoble, il était situé **dans une multiprise**

Sûrement installé pendant une perquisition plus tôt dans le mois

Août 2018

https://nantes.indymedia.org/posts/42509/

Conseils

Ne parlez pas de choses ultra confidentiel dans des lieux militants, chez un.e militant.e et dans la voiture d’un.e militant.e

Variez régulièrement les lieux de réunions ultras confidentielles

Comment est ce que la police peut vous écouter lors d’une réunion ?

Lieu sonoriser (sur écoute)

Quelqu’un présent dans la réunion

Piratage d’un téléphone portable

Quel type de personnes peuvent corrompre la sécurité des informations d’une réunion ?

Quel type de personnes peuvent corrompre la sécurité des informations d’une réunion ?

Policier en civil

Policier infiltré

Indic

Militant mal sécurisé

Policier/indic

Présent lors du debriefing de l'action « Grand péril express »

les manifestations et actions de désobéissance civile, jugées « stériles », sont enclins à basculer dans la radicalité et à rejoindre les SLT. Ainsi Prénom NOM, autre militante originaire du groupe XR Paris/Ile de France, a progressivement pris ses distances avec le groupe écologiste pour s'investir pleinement dans les actions plus offensives et engagées, proposées par le mouvement des SLT et s'afficher aux côtés de Prénom NOM lors de l'action Grand Péril Express (prises de parole lors de débriefings). Le profil de Prénom NOM illustre également ce type de parcours. Après un passage sur l'ex-ZAD de NDDL durant l'été 2018, elle a fondé le collectif inter-faculté Désobéissance écoloParis, avant de rejoindre le groupe Extinction rébellion la Rochelle, puis d'occuper les

https://reporterre.net/IMG/pdf/soule_vements.pdf

Policier en civil

Renseignements territoriaux

Ne vont pas tellement attirer l’attention et pas tellement parler

Ça arrive souvent qu’ils assument être flics

Policier infiltré

Exemple : Mark Kennedy, actif de 2003 à 2010, dont en France dans le collectif militant de Tarnac

Ont des relations amoureuses avec des militantes

Font des choses illégales avec vous

Ont toujours été flics

https://basta.media/Ces-apprentis-James-Bond-qui
https://www.lemonde.fr/blog/moreas/2016/04/28/la-justice-secrete-indic-infiltre-repenti-collaborateur/

Indics (aka source humaine)

D’anciens militants, attrapés un jour et qui encourt une lourde peine de prison et décide de devenir indic

D’anciens militants qui veulent se faire de l’argent

Peuvent être payé en espèce par la police (loi Perben II) et avoir des réductions de peine ou des annulation des poursuites

Très présent en ZAD

https://fr.wikipedia.org/wiki/Indicateur_(police)
https://www.lemonde.fr/blog/moreas/2016/04/28/la-justice-secrete-indic-infiltre-repenti-collaborateur/

Une militante mal sécurisé

Compte rendu rendu trop publique

Compte rendu obtenu a posterieuri lors d’une perquisition

Conseils

Le plus importants est de ne pas soupçonné tout le monde tout le temps

A moins qu'il y ai des preuves très concrètes, ne pas se tirer dans les pattes

Cloisonner l'information

Avoir des procédures de sécurité précise, claire et publiques avec potentiellement des sanctions

Exemple : ZAD, interdiction d'entrer dans la tente de quelqu'un d'autre sans son accord sinon exclusion

Former vos militantes !

Comment est ce que la police peut vous écouter lors d’une réunion ?

Lieu sonoriser (sur écoute)

Quelqu’un présent dans la réunion

Piratage d’un téléphone portable

Piratage d’un téléphone portable

Dans le cadre d’une enquête, la police peut pirater votre téléphone portable ou votre ordinateur afin de regarder ce qu’il y a dedans : vos conversations Signal, Telegram, historique de recherche sur internet…

Elle n’a pas le droit d’utiliser votre micro ou votre caméra (Loi d’orientation de la justice 2023)

Piratage d’un téléphone portable

La police n’a pas le droit de vous regarder et de vous écouter mais qu’est ce qui l’en empêche ?

« Eric Dupond-Moretti soulignait que le déclenchement à distance d'appareils connectés est déjà utilisé par "les services de renseignement", sans l'autorisation du juge, qui devait être ici indispensable »

Le Monde

SOCIÉTÉ

Tarnac : la justice enquête sur des écoutes illégales menées avant l'affaire du sabotage

La juge instruit sur le chef "d'atteinte au secret des correspondances" et "à l'intimité de la vie privée".

Par Laurent Borredon

Publié le 09 janvier 2012 à 11h36, modifié le 24 février 2012 à 13h04 · Lecture 4 min.

Faille de sécurité : qu’est ce que c’est

Pour installer un logiciel espion (spyware) dans votre téléphone il faut trouver une faille de sécurité

franceinfo:

Cybersécurité : les ministres français invités à désinstaller les applications de messagerie comme Whatsapp, Signal ou Telegram

Selon Elisabeth Borne, ces applications de messageries instantanées "ne sont pas dénuées de failles de sécurité et ne permettent donc pas d'assurer la sécurité des informations" échangées.

Faille 0 day

Je trouve une faille de sécurité

Prévenir le concepteur	**Faire de l'argent en exploitant cette faille (faire un exploit)**	**Revendre la faille à une entreprise qui fait de l'exploitation de faille**
Rémunération sous forme de bug bounty (peut se compter en millions d'euro) + éthique	Possibilité de faire beaucoup d'argent illégalement	NSO = entreprise israellienne qui fournit un logiciel permettant a des entités éthatiques de surveiller leur population

Quelqu’un peut il nous parler de Pegasus ?

Pegasus

Logiciel Israëlien permettant d’infecter des téléphones portables découvert le 18 juillet 2021

Coûte extrêmement chère

Exploite des failles de sécurité

Ce logiciel aurait permis d'espionner les numéros d'au moins 180 journalistes, 600 hommes et femmes politiques, 85 militants des droits humains ou encore 65 chefs d'entreprise de différents pays

https://www.arte.tv/fr/videos/106169-001-A/pegasus-un-espion-dans-votre-poche/

Faille 0 day

3 catégories :

- Faille de sécurité lié à l’appareil (Iphone11, Samsung Galaxy S22...)

- Faille de sécurité lié au système d’exploitation (Android 10, iOS 11...)

- Faille de sécurité lié à une application (Whatsapp, Messenger...)

Faille 0 day : prix d’une faille

Selon le prérequis et ce que ça permet de faire, les prix varies : ça peut aller jusqu’à plusieurs millions d’euros

Exemple : en 2021, une faille « zero click RCE » (remote code execution) sur WhatsApp (2,5 Millions d’utilisateurices) coûtait 1,7 million de dollars

En 2016, NSO Group facturait 650 000$ pour hacker 10 smartphones, 1 450 000$ pour 100 smartphones

Le contrat de NSO avec l’Arabie saoudite s’élèverait à lui seul à 55 millions de $

Faille 0 day : prix d’une faille

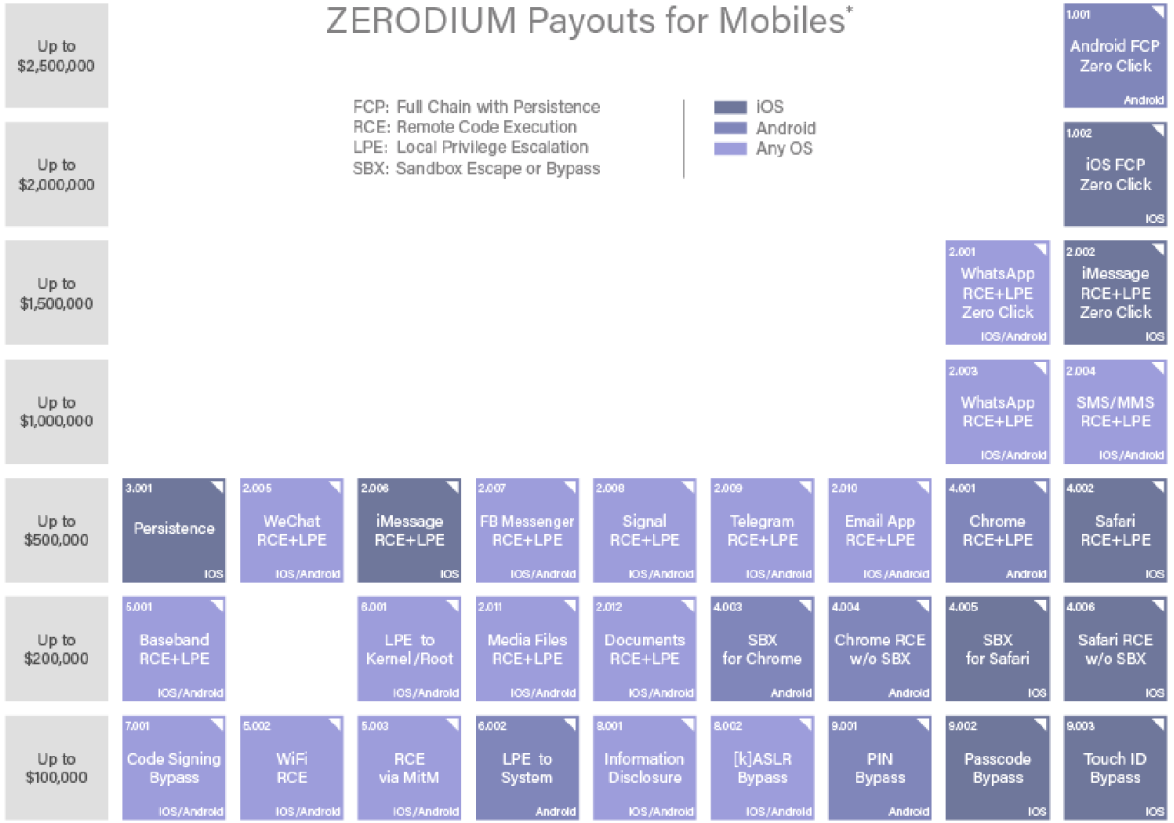
La puissance de la faille correspond à :

Les prérequis :
- que la personne est tel ou tel application
- avoir seulement besoin du numéro de téléphone
- avoir le téléphone en physique et dévérouillé
- que la cible clique sur lien et accepte de télécharger quelque chose
…

Les choses que ça permet de faire :
- pouvoir lire les messages de l’application
- pouvoir lancer du code sur le téléphone à distance (RCE)
- pouvoir voir en temps réel ce qui est sur l’écran du téléphone
…

Pegasus utilisait des failles où il suffisait d’avoir le numéro de téléphone d’une personne pour la pirater et pouvoir avoir accès à tout le téléphone

Marché de failles : Zerodium



** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/09 © zerodium.com

Faille matériel 0 day : solutions

Avoir un téléphone dernière génération

Avoir un téléphone qui prend la sécurité du matériel au sérieux : Google Pixel, Iphone

Faille OS 0 day : solutions

Mise à jour régulières de votre OS

Avoir le dernier OS mais surtout un OS qui a toujours des mises à jour de sécurité

Utiliser GrapheneOS

Faille application 0 day : solutions

Mise à jour régulières de vos applications

+ vous avez d’applications + vous avez de failles de sécurité

+ vos applications ont des droits sur votre téléphones + vous avez de failles de sécurité

Avoir des applications validées par la street !

Installation spyware durant une garde à vue (GAV)

Des failles de sécurité qui permettent de déverrouiller un smartphone qu'on a physiquement entre les mains ne coûtent vraiment pas très chère
Un fois qu'on a votre portable déverrouiller entre les mains, il est très facile d'installer un spyware

Conseil :

Changer de portable si il passe entre les mains de la police lors d'une GAV

Ne laissez pas votre portable sans surveillance

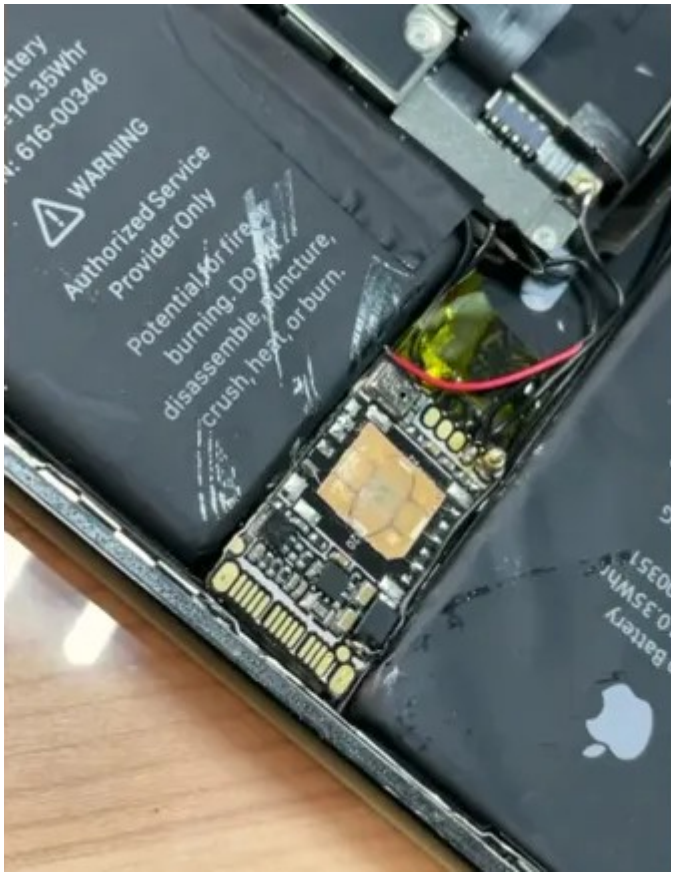
Téléphone compromis

Microphone et traceur GPS installé en physique dans un iPhone

Installé durant une détention de 1 semaine

En Russie

Décembre 2020



https://meduza.io/en/feature/2021/01/14/we-found-a-wiretap

Porte dérobée

Faille de sécurité installer exprès par le concepteur ou installer par la police lors d'une GAV

Exemple : le gouvernement chinois pourrait obliger Samsung à mettre des failles de sécurité dans leurs téléphones intelligents afin de pouvoir surveiller sa population

Darmanin : « Hier encore, les écoutes téléphoniques classiques nous renseignaient sur la grande criminalité et le terrorisme. Aujourd'hui, les gens passent par Telegram, par WhatsApp, par Signal, par Facebook (…) Ce sont des messageries cryptées (…) On doit pouvoir négocier avec ces entreprises ce que vous appelez une "porte dérobée". On doit pouvoir dire : "Monsieur Whatsapp, Monsieur Telegram, je soupçonne que M. X va peut-être passer à l'acte, donnez-moi ses conversations." »

Porte dérobée concepteur : solutions

Choisissez bien vos applications, OS, matériels...

Exemple :

- Avoir un OS libre comme 

- Avoir un téléphone de marque chinoise (Huawei, Xiaomi, Honor...)

- Ne pas utiliser des applications mainstreams capitalistes propriétaire

Ayez un maximum de choses open-source car c’est beaucoup plus dure de cacher une porte dérobée

Piratage de votre appareil : solutions générales

Déconnecter le micro (difficile) ou ajouter un assourdisseur (pâte à fixe)

Mettre un cache sur la webcam

Ne pas avoir son portable avec soit lorsque l’on parle de choses incriminantes

Un portable en mode avion ne change rien

Éteindre son portable réduis les risques mais ne les supprime pas totalement

Comment est ce que la police peut vous écouter lors d’une réunion ?

Lieu sonoriser (sur écoute)

Quelqu’un présent dans la réunion

Piratage d’un téléphone portable

Conclusion

Écoute : micro-ondes ?

Ça ne permet sûrement pas d’éviter les écoutes car :

- selon le microphone de votre portable, on vous entendra toujours
- possibilité d’enregistrer puis d’envoyer les enregistrement une fois sortit du micro-ondes
- un micro-ondes n’est pas fait pour arrêter les ondes d’un portable

Bornage

Qu’est ce qui permet de savoir que vous êtes sur place ?

Qu’est ce qui permet de savoir que vous êtes sur place ?

Des caméras

Les téléphones portables

Qu’est ce qui permet de savoir que vous êtes sur place ?

Des caméras

Les téléphones portables

Caméra

Le site « Ears and Eyes » a recensé 28 caméras dans les 20 dernières années (6 en France)

Principalement devant des lieux militants, visant les entrées du lieu

Caméra

Caméras situées devant l’espace autogéré des Tanneries à Dijon (dernière ADR) et devant le quartier libre des Lentillères à Dijon aussi

De ~2019 à 2022

Posé par la police

Filmant l’entrée des lieux

https://dijoncter.info/surveillance-policiere-des-cameras-decouvertes-aux-tanneries-et-aux-lentilleres-4299

Caméra

Une caméra retrouvé à Sevreau (Deux-Sèvres) devant le domicile du père de Julien Leguet, porte parole de « Bassines non merci »

Mars 2022

Posé par la police

Filmant l’entrée du lieu

https://france3-regions.francetvinfo.fr/nouvelle-aquitaine/deux-sevres/niort/julien-le-guet-leader-du-mouvement-bassines-non-merci-espionne-par-une-camera-de-surveillance-2503959.html

Caméra : solutions

Ne faites pas vos briefing dans des lieux militants

Si vous allez dans un lieu militant, ne vous garer pas en face et cachez votre visage

Essayez d’éviter les caméra publiques (https://sunders.uber.space/)

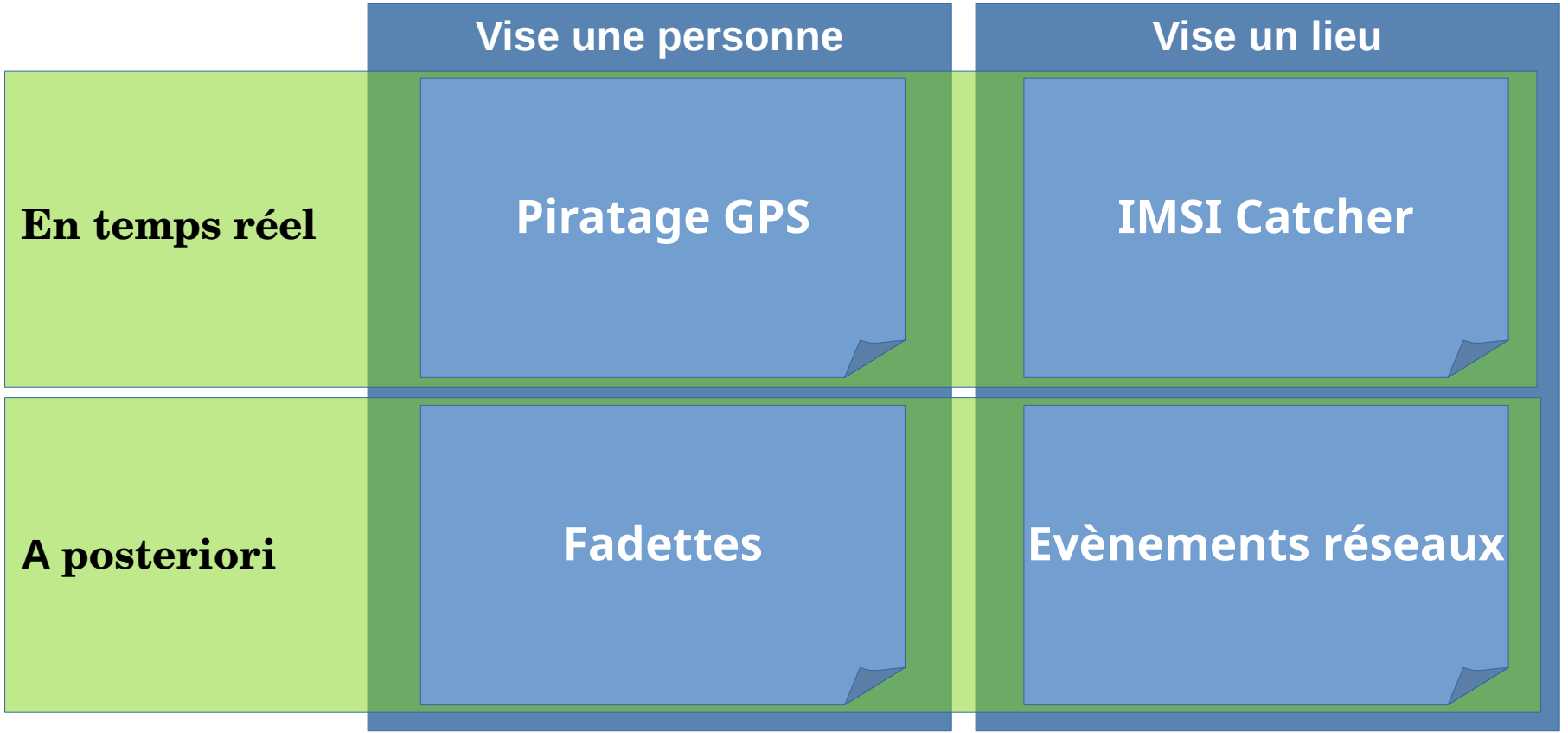
Qu’est ce qui permet de savoir que vous êtes sur place ?

Des caméras

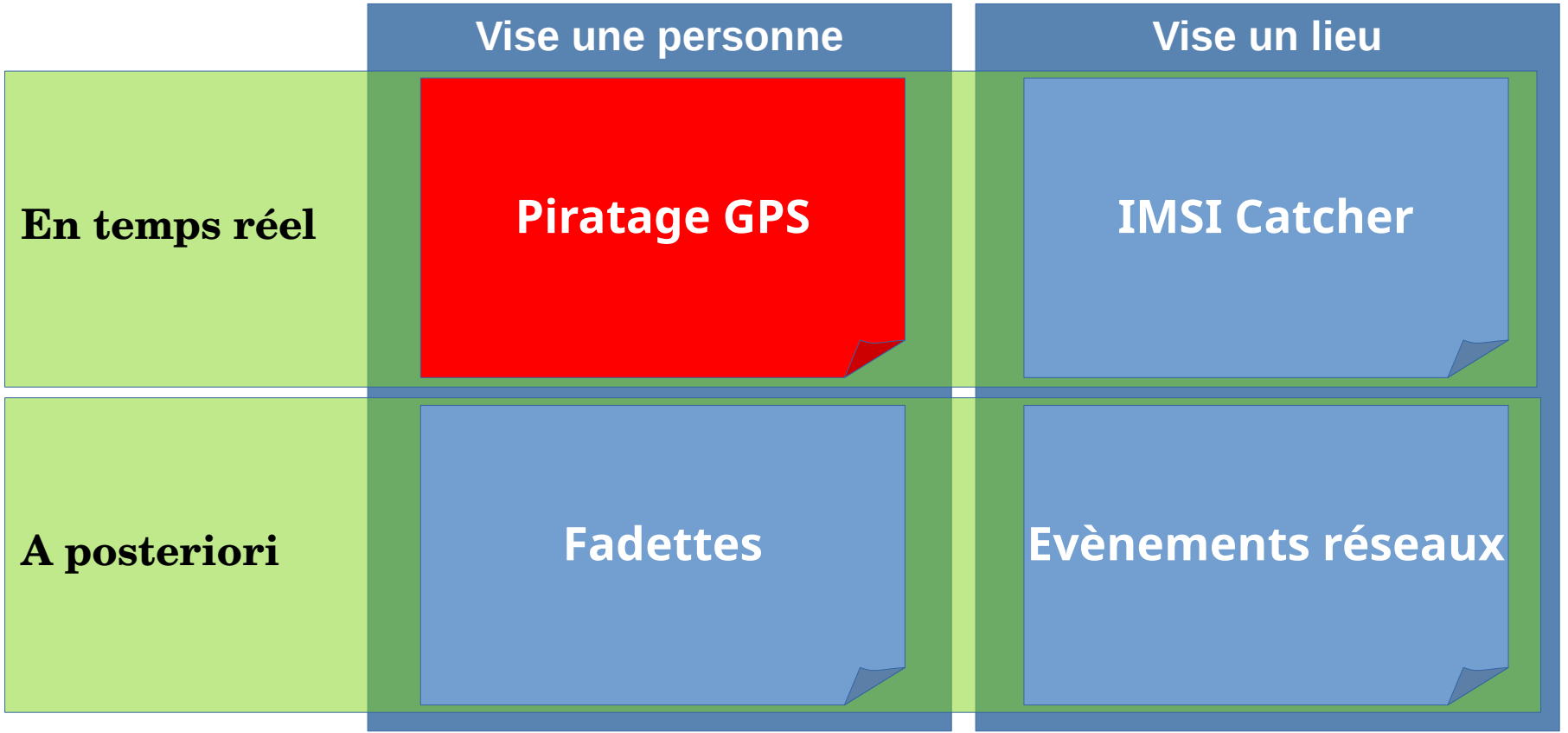
Les téléphones portables

Comment votre téléphone peut prévenir la police que vous êtes sur place ?

Comment votre téléphone peut prévenir la police que vous êtes sur place ?



Comment votre téléphone peut prévenir la police que vous êtes sur place ?



Bornage : piratage GPS

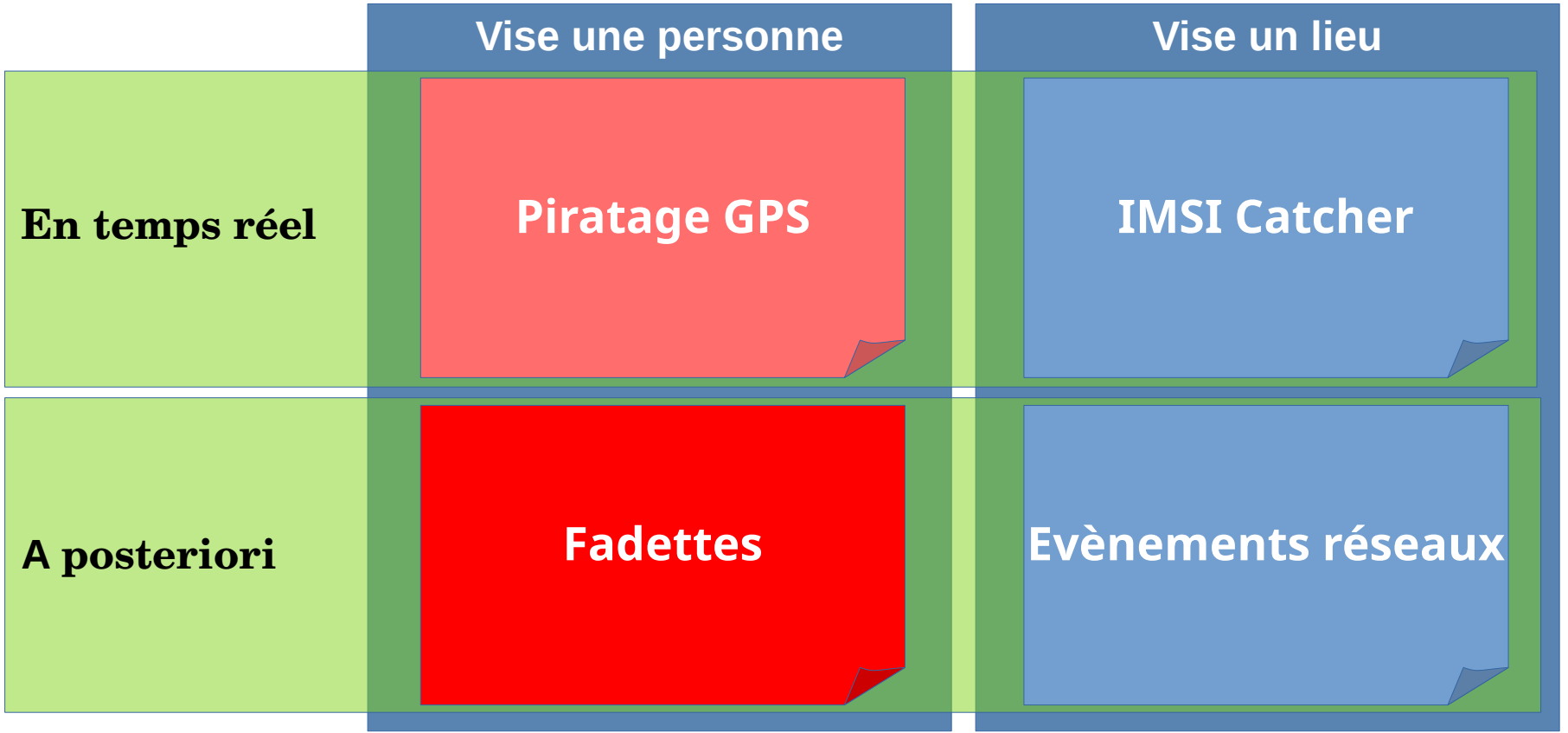
On pirate votre portable pour utilisé sa fonction GPS (Loi d’orientation de la justice 2023)

Comme précédemment nécessite une faille de sécurité

Peut être précis au mètre près

Fonctionne en mode avion et probablement pas lorsque le portable est éteint

Comment votre téléphone peut prévenir la police que vous êtes sur place ?



Bornage : fadettes

Liste des appels, SMS et DATA envoyés et reçus avec la localisation de l’antenne relais

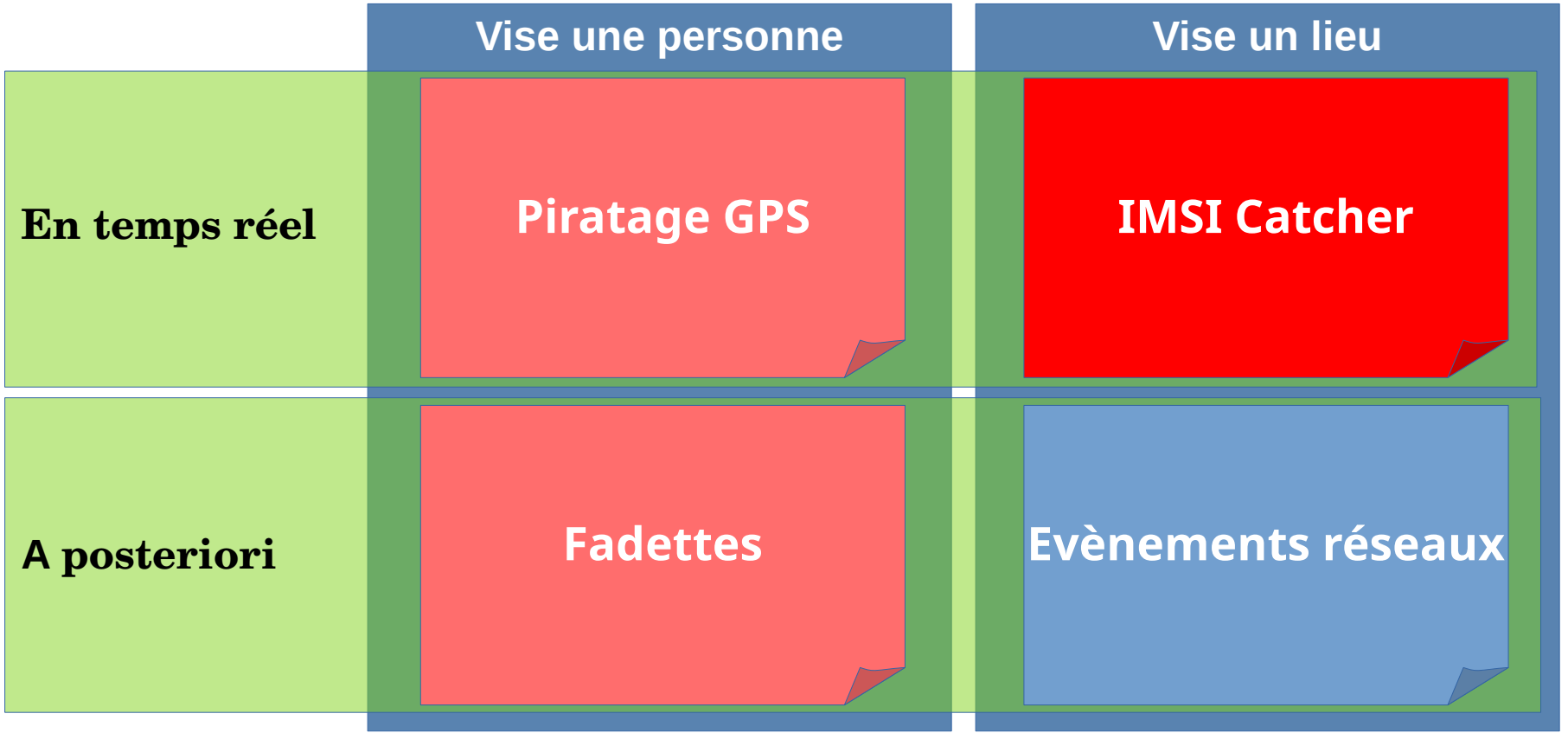
La précision varie : de 1 patté de maison en ville à plusieurs kilomètres à la campagne

Obligation des opérateurs de garder ces données pendant 1 an

Permet de savoir où vous étiez et des fois qui vous êtes

Première chose regardé par la police en cas d’enquête → garder ses habitudes

Comment votre téléphone peut prévenir la police que vous êtes sur place ?



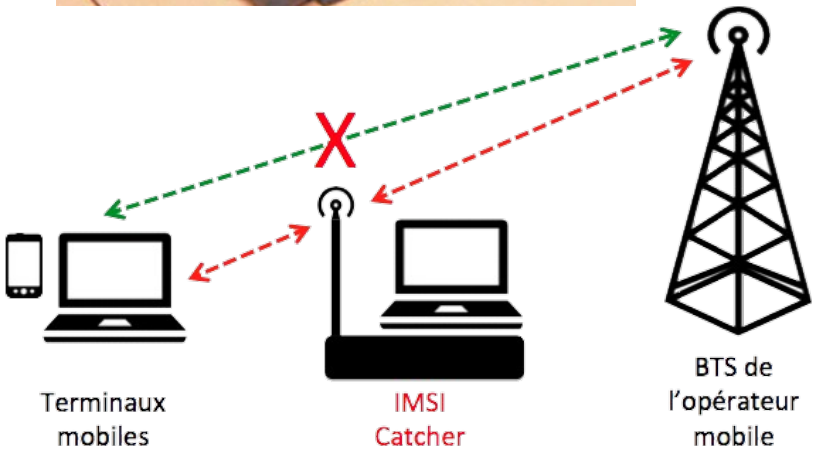
Bornage : IMSI Catcher

Dispositif permettant de savoir quels portables sont dans les « environs » en direct

Très précis

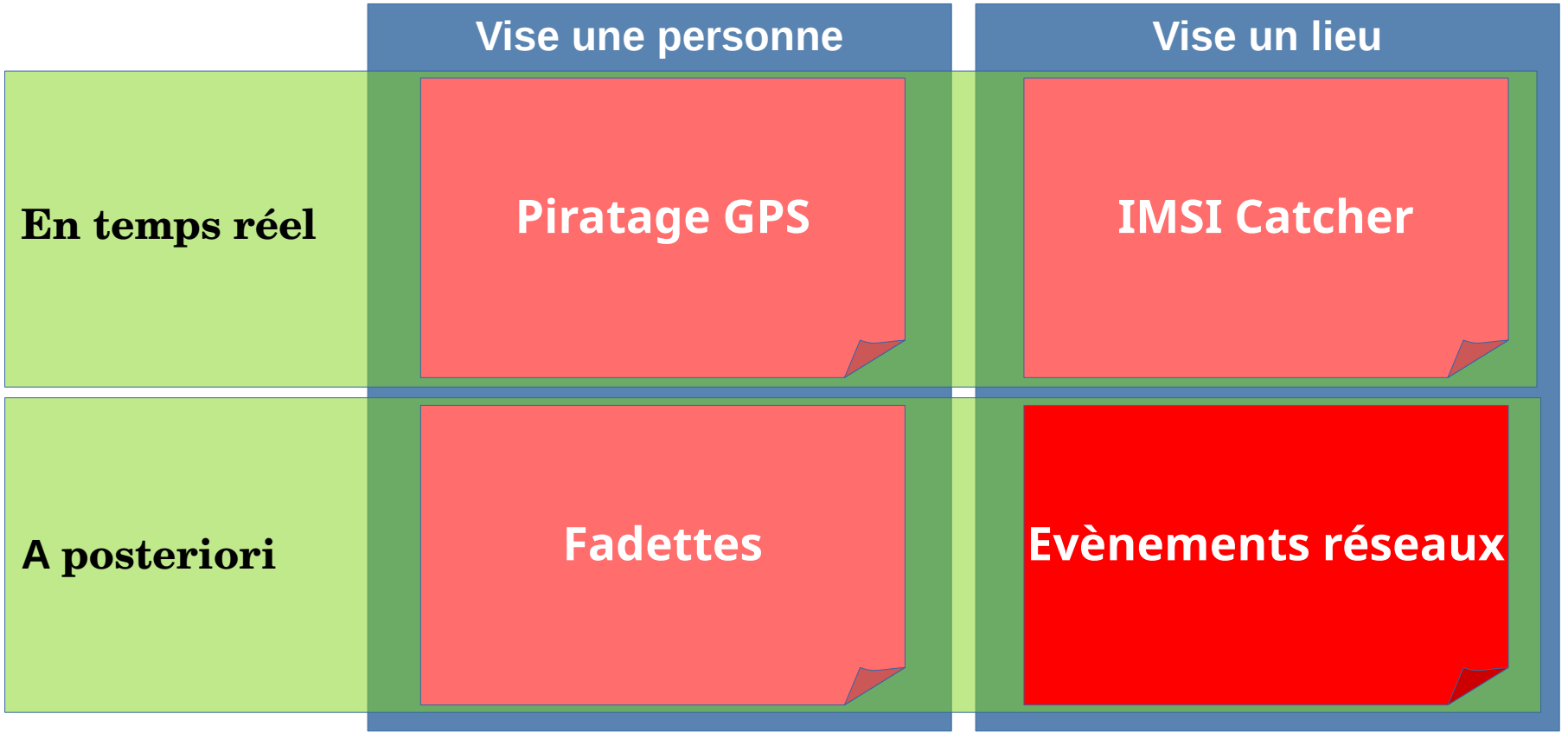
Déployer en amont

Exemple de moment où il y a des IMSI catcher :
- Sainte Soline
- Jour d'affrontement en ZAD
- Pour decouvrir le deuxième portable d'une militante



Brochure : Affaire « Lafarge » Les moyens d'enquêtes utilisés et quelques attentions à en tirer
https://www.lemonde.fr/pixels/article/2015/03/31/que-sont-les-imsi-catchers-ces-valises-qui-espionnent-les-telephones-portables_4605827_4408996.html

Comment votre téléphone peut prévenir la police que vous êtes sur place ?



Bornage : évènements réseaux

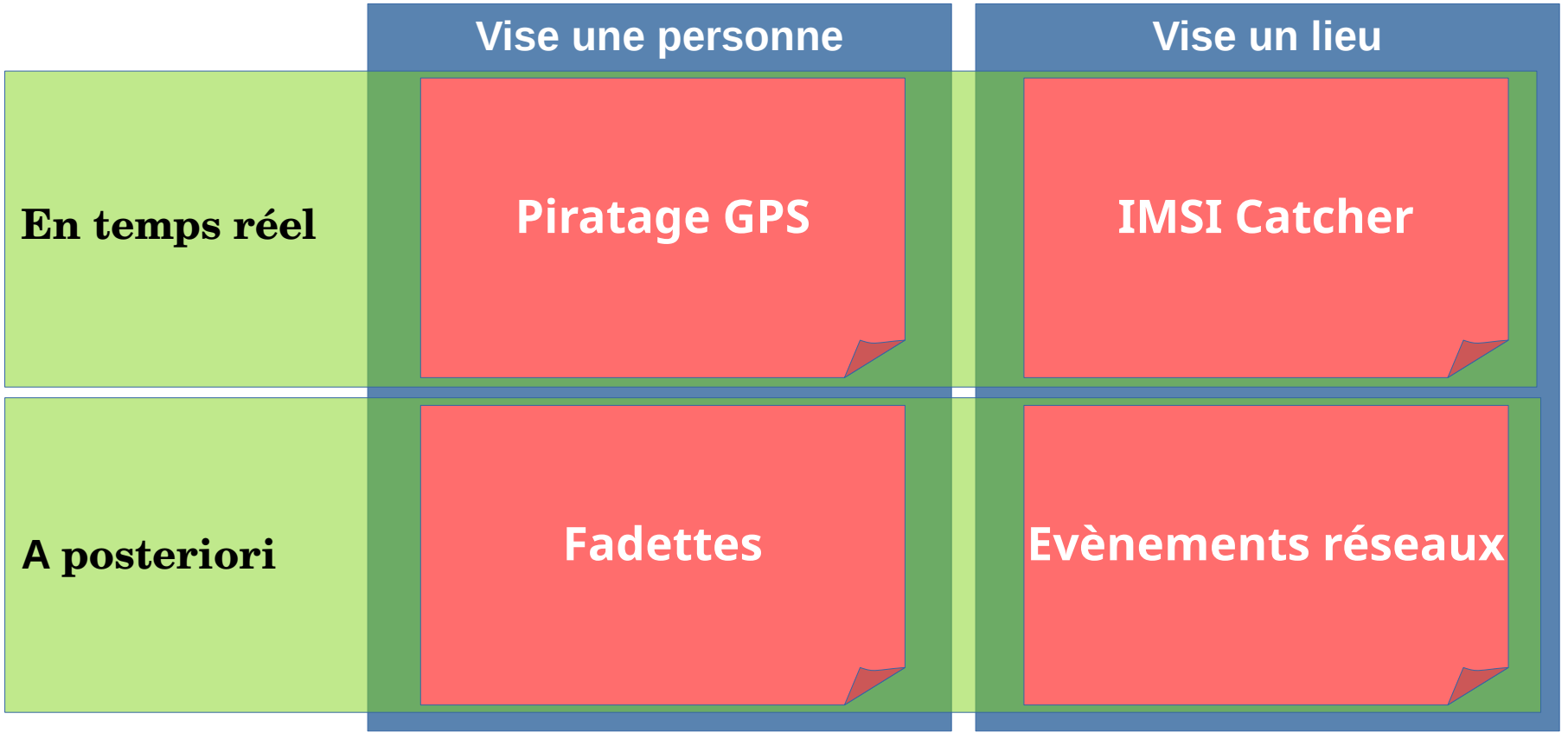
On demande à une antenne quels téléphones portables sont passés dans le coin et ce qu’il y on fait

Contrairement aux fadettes, marche même si on ne reçois et envois rien

Contrairement à l’IMSI catcher, est utilisé a posteriori

Précisions supérieur aux fadettes

Comment votre téléphone peut prévenir la police que vous êtes sur place ?



Bornage : micro-ondes ?

Tout les portables s’éteignent en même temps à un endroit précis
Cela peut permettre à la police :
- De savoir qui était à la réunion
- De savoir quand et où était la réunion

Un micro-ondes n’est pas fait pour arrêter les ondes d’un portable

C’est plus dangereux que de ne rien faire du tout

Bornage : solution

Téléphone portable allumé <

Téléphone portable en mode avion <

Téléphone portable éteint <

Téléphone portable sans batterie <

Téléphone portable dans une cage de faraday <

Pas de téléphone portable

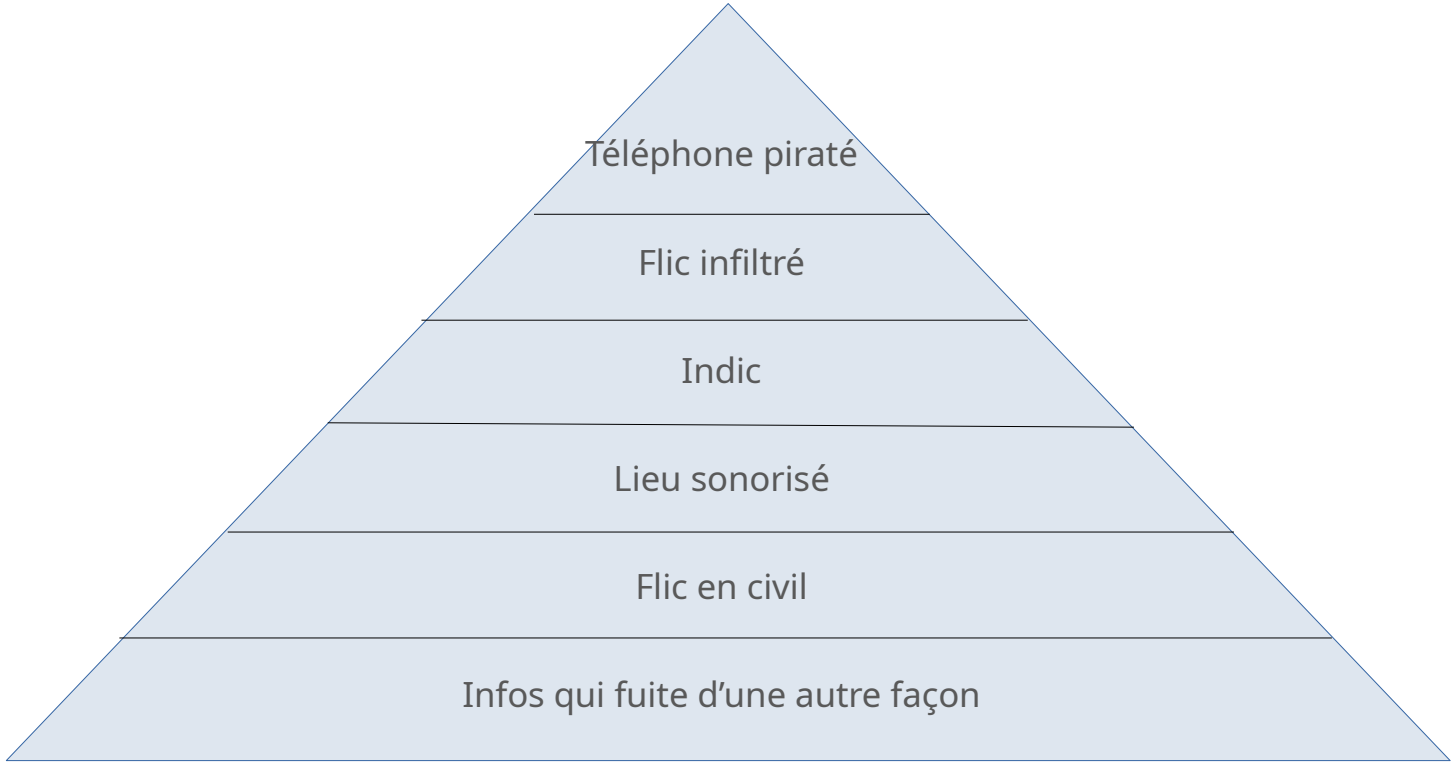
Possibilité de le mettre mode avion + wifi : le mettre en mode avion bien avant d’arriver sur place

Réunion ~= action

Ce que l’on a vu pour les réunions est applicable aussi en action + risque de perquisition du téléphone

→ Ne prenez jamais votre portable en action !

Réduction des risques



Récapitulatif

Un portable en réunion ce n’est pas très dangereux si il est en mode avion depuis bien avant d’arriver au lieu mais le plus sécur c’est de toujours venir sans portable

C’est contre productif durant une réunion de demander aux gens de se mettre en mode avion, d’éteindre leur téléphone ou de le mettre dans une boite : c’est déjà trop tard
→ vaut mieux leur demander de le mettre en silencieux

N’éteignez pas votre portable devant le lieux avant de rentrer non plus

Évitez les lieux militants pour les formations ultra confidentielles

Organiser des formations vers chez vous !

Des questions ?