COMMENT ORGANISER UNE ACTION DIRECT?

CONTRE LE MACHINE DE GUERRE SIONISTE: UN GUIDE PRATIQUE

BIENVENUE

Bienvenue et merci d'être ici. Ce guide pratique vous aidera à organiser votre propre action directe contre la machine de guerre sioniste en Belgique. Lisez attentivement ce guide et bonne chance!

LA SÉCURITÉ EST IMPORTANTE.

Principes fondamentaux de la sécurité numérique :
→ Utilisez toujours le navigateur Tor
→ Utilisez VPN pour faire vos recherches
→ Ayez des mots de passe solides sur tous les outils que vous utilisez et faites en sorte que ceux-ci ne soient jamais sauvegardés automatiquement sur votre ordinateur (mémorisez-les!).

Encore plus important en termes de sécurité: ne vous vantez pas de ce que vous prévoyez de faire ou de ce que vous avez fait. N'en parlez pas dans des lieux publiques comme des bars ou des soirées, même si vous êtes entre ami.es. Interpellez vous entre vous si vous êtes témoin de ce comportement de la part d'un.e membre de votre groupe affinitaire.

ETAPE 1 - FORMER UN GROUPE AFFINITAIRE

Un groupe affinitaire est un groupe autonome qui entreprend des actions. Il est crucial que vous n'invitiez que des personnes que vous connaissez bien et en qui vous avez confiance dans votre groupe affinitaire. Plus le groupe est petit, plus il est sécurisé: un nombre idéal serait de 4 à 8 personnes, mais certaines actions peuvent être menées avec 2 ou 3 personnes.

Une fois votre groupe formé, donnez-lui un nom. Vous pouvez utiliser le nom d'une personne qui s'est battue pour la liberté de la Palestine, un jeu de mot ou n'importe quoi qui vous semble approprié.

Communiquez entre vous via Signal. Lisez attentivement les consignes de sécurité numérique et la fin de ce manuel pour utiliser Signal en toute sécurité.

Maintenant créez une adresse mail sécurisée comme ProtonMail ou d'autre services de mails cryptés. Cette étape est indispensable pour pouvoir envoyer les informations de votre action à Stop Arming Israel.

Vous trouverez plus de détails à ce sujet plus loin dans ce guide.

ETAPE 2 - CHOISISSEZ UNE CIBLE

Maintenant que vous avez votre groupe, choisissez une cible. Rendez-vous sur www.stop-arming-israel-belgium.com pour consulter une liste liées à OIP/Elbit ou impliquées d'une autre manière dans la production ou le transit d'équipements militaires de la Belgique vers Israël. Cette liste est régulièrement mise à jour !

Toutes ces cibles sont complice du génocide. En augmentant suffisamment le coût de leur coopération avec l'industrie de guerre israélienne via nos actions, nous les forçons à reconsidérer cette coopération.

Lorsque vous choisissez votre cible, prenez en compte votre lieu de résidence pour simplifier la plannification et le repérage ainsi que pour économiser sur le coût des transports.

Vous êtes basé.es en France ? Vous trouverez ici une carte (non-exhaustive) avec plus de 170 sites de fabricants d'armes français complice d'Israël:

ETAPE 3 - PRÉPARATION DE L'ACTION

1. REPÉRAGE

Lors de la préparation d'une action, il est crucial de bien connaître votre cible et d'y faire du repérage. Faites-le le plus discrètement possible afin de ne pas vous faire attraper sur le coup ou vous faire identifier après l'action. Adaptez votre comportement et votre tenue en fonction de la cible.

Assurez-vous que votre téléphone soit toujours en mode avion lorsque vous faites du repérage pour que vous ne puissiez pas être identifié.es plus tard par le bornage de votre téléphone.

Si votre cible est dans le centre-ville, il n'y a rien de suspect dans le fait de vous prommener avec un.e ami.e ou seul.e et de prendre des photos du lieu. Mais si vous marchez dans une zone industrielle avec une perche à selfies, vous allez certainement attirer l'attention.

Si vous vous rendez dans des zones plus rurales, vous pouvez par exemple prendre un chien avec vous. Ou encore mettez des vêtements de sport et allez courir ou faire du vélo. Faites en sorte d'avoir une histoire convaincante sur la raison de votre présence au cas où une personne vous le demande (vous êtes à la recherche d'un chat perdu, vous faites du géocaching etc...).

Vous pouvez également faire du repérage en voiture, mais faites attention à ne passer devant la cible qu'une seule fois et récoltez toutes les informations dont vous avez besoin lors de cet unique passage afin que votre plaque d'immatriculation n'apparaissent pas plusieurs fois devant les caméras.

Lorsque vous faites du repérage, c'est une bonne chose de prendre des photos mais faites attention aux points suivants:

- Prenez vos photos directement dans Signal. De cette manière elle ne laisseront pas de traces numériques sur votre téléphone. Rappel: votre téléphone doit être en mode avion. Les photos seront envoyées dès que vous retrouverez une connexion.
- N'attirez pas l'attention en prenant des photos ou vidéos. Soyez rapides et maintenez votre téléphone dans une position qui montre pas de manière évidente que vous êtes en train de photographier. Vous pouvez par exemple marcher, passer en vélo ou en voiture avec votre téléphone en train de filmer plutôt que de rester immobile. Ou bien faites semblant de prendre en photo quelque chose d'autre avec la cible en fond.

Si vous faites votre repérage longtemps avec l'action, prévoyez un deuxième passage juste avant l'action pour vérifier qu'il n'y a pas eu de changements majeurs entre-temps.

2. ONLINE RESEARCH

Avant d'aller voir la cible en personne il est toujours intéressant de faire du repérage en ligne dans un premier temps. Cela vous donnera une meilleure idée de ce que vous pourriez faire pendant votre action et donc de ce à quoi vous devrez prêter attention lors de votre repérage en personne, sans prendre trop de risques.

En plus de Google Maps et Google Earth, utilisez des services de cartes tels que Bing et Mapillary, qui fournissent parfois des informations additionelles ou complémentaires. Si possible, faîtes ça avec un navigateur sécurisé et un VPN. Google Maps ne fonctionne parfois pas avec Tor mais dans tous les cas utilisez un navigateur dans lequel vous n'êtes pas connecté à un compte Google.

Ne vous reposez pas exclusivement sur les informations que vous trouvez en ligne car les entreprises changent constamment des choses et les cartes en ligne ne sont pas toujours à jour. Rien ne remplace une visite en personne pour vous préparez correctement.

DÉCOUVREZ CE QU'IL FAUT RECHERCHER À LA PAGE SUIVANTE.

Les informations importantes à relever

Les agents de sécurité - Combien y en a-t-il ? Sont-iels stationaires ou mobiles ? A l'intérieur ou à l'extérieur ? Que surveillent-iels ? Que peuvent-iels voir ? Quelles rues ? Quels sont leurs horaires ? - Il vaut mieux éviter les horaires de changement de garde car cela veut dire qu'il y a plus de gardes sur site. Les équipes de sécurité restent-elles à l'intérieur du site ou bien gardent-elles les entrées depuis l'extérieur ?

Les travailleureuses - Combien de personnes semblent travailler sur le site ? Pouvez-vous compter les voitures ? Quels sont les horaires de travail ? Y a-t-il des moments ou beaucoup de personnes arrivent/quittent les lieux ? Y a-t-il une présence 24/7 ?

Les caméras - Positions ? Nombre de caméras ? Que surveillent-elles et que peuvent-elles voir ? Il est souvent impossible d'agir en dehors du champ de vision des caméras, il faut donc absolument être anonyme et non-indentifiable.

Les entrées - Combien de points d'accès vers le site ou un bâtiment y a-t-il ? Prnez aussi note des sorties de secours. Quels types de serrures sont installées sur les portes et comment pourriez-vous les ouvrir si nécessaire ?

Les environs - Qu'y a-t-il proche de la cible ? Du voisinage ou d'autres types de lieux ? Les batiments alentours ont-ils des gardes ? Ou encore à quels moments de la journée des personnes sont-elles présentes dans les bâtiments environnants ?

Les alarmes - Y a-t-il une alarme ? Qu'est-ce qui pourrait la déclencher ? Tout ce qui pourrait déclencher une alarme doit être gardé pour la fin.

La police - Où sont les comissariats les plus proches ? Y a-t-il des patrouilles dans la zone ? Des voitures banalisées ? Des patrouilles piétonnes ? Essayez d'avoir une estimation du temps de réponse de la police.

Le parking - Où pouvez-vous vous garer avant, pendant et après l'action ? Il est important de trouver des lieux de parking qui ne sont pas sous vidéosurveillance et qui ne demandent pas de ticket de parking

Les transports - Pouvez-vous vous rendre à votre cible en transports en commun ? Y a-t-il des endroits sans caméras (un parc, un terrain ouvert...) où vous pourriez vous changer afin de ne pas être reconnus via les caméras des transports ?

Le plan de sortie - Comment pouvez-vous quitter le lieu sans être vu par des caméras ? Y a-t-il des pistes cyclables, des champs ou des bois par lesquels vous pourriez disparaître sans être suivi.es ? Y a-t-il des lieux publics où vous pourriez vous mêler à la foule ? Assurez-vous d'avoir plusieurs plans de sortie.

2. METTEZ EN PLACE UNE ÉQUIPE D'ASSISTANCE JURIDIQUE

Pourquoi une équipe de soutien juridique ?
L'objectif d'une équipe de soutien juridique est de garantir que les activistes arrêté.es ou poursuivi.es ne soient pas livré.es à eux-mêmes et que leurs droits soient respectés. En outre, une équipe de soutien juridique sert à garder une vue d'ensemble, à informer les ami.e.s et la famille si nécessaire et à organiser des campagnes de soutien, de financement participatif et de communication.

Comment organiser un soutien juridique ?
Selon l'action, l'expérience ou les besoins des activistes, votre soutien juridique peut être aussi petit ou aussi grand que vous le souhaitez. Vous trouverez ci-dessous un plan détaillé des possibilités, mais celui-ci ne sera sans doute pas nécessaire pour chaque action. A minima, cela consiste à informer une personne extérieure à l'action que vous allez mener une action. Cette personne peut vérifier que vous êtes rentré.e chez vous dans les 24 heures et peut informer les personnes concernées.

Pour une petite action, une équipe de soutien juridique peut se composer d'une ou deux personnes qui restent chez elles ou dans un lieu sûr, et suivent l'action à distance. L'objectif du soutien juridique est d'être bien préparé.es avant, pendant et après l'action aux éventuelles conséquences juridiques et au stress émotionnel que cela peut entraîner.

Vous trouverez ci-dessous un bref plan par étapes sur comment organiser un soutien juridique pour une action vous-mêmes.

ETAPE 4: PLANNIFIER VOTRE ACTION

1. TYPES D'ACTIONS

Maintenant que votre repérage est effectué, il est temps de développer et raffiner votre plan. Il est important d'être créatif.ves pour que notre résistance reste efficace. Lorsque vous préparez votre action c'est une bonne chose de définir clairement avec votre groupe ce que vous voulez accomplir avec votre action.

Voici quelques exemples de différentes actions en soutien à la Palestine que des groupes ont effectuées. Si vous avez peu d'expérience, il vaut mieux commencer avec des actions simples et évoluer graduellement vers des actions plus complexes. Toutes les idées qui rentrent dans le consensus d'action sont possibles. Voici quelques suggestions pour vous lancer...

- **Redécorer votre cible:** les extincteurs peuvent être détournés et remplis de peinture rouge sang, projettant alors de grandes quantités de peinture lorsqu'on les déclenche. Cela permet de recouvrir de peinture de grandes surfaces en peu de temps. Parfait pour une action rapide.
- **Peindre votre message:** faire un tag avec une bombe de peinture peut aussi être rapide tant que vous n'essayez pas d'écrire une longue histoire sur les murs de la cible.
- **Bloquer la cible:** vous pouvez bloquer les entrées d'un bâtiment avant que les travailleureuses n'arrivent, de sorte à ce qu'iels ne puissent pas effectuer leurs tâches. Ou bien empêcher d'entrer ou de sortir les camions qui contiennent les matériaux nécessaires aux activités de l'entreprise. Le blocage peut être fait avec votre corps (ce qui implique de grande chances d'être arrêté.es et potnetiellement identifié.es) ou avec du matériel divers; un cadenas à vélo autour d'un portail, un gros trou dans la route pour empêcher les camions de passer, de la colle dans les serrures de portes etc.

Voyez grand: les tactiques données ici sont des exemples d'actions passées, ne soyez pas effrayé.es d'innover ! Ne vous limitez pas à ce qui existe déjà et demandez-vous à chaque brainstorm: que pourrais-je faire pour être encore plus créatif.ve ?

2. PRÉPAREZ-VOUS À D'ÉVENTUELLES CONSÉQUENCES JURIDIQUES

Inschatting maken en informeren van de risico's
Op basis van je actieplan kan je een inschatting maken van de juridische risico's die jullie eventueel nemen. Hiervoor kan je je onder andere baseren op het juridische risico's document en het strafwetboek en indien je specifieke vragen hebt, kan je ook het legal team van Stop Arming Israel contacteren. Het legal team bestaat uit mensen met actie-ervaring en ervaring in legal teams, maar niet noodzakelijk juristen of advocaten. Ze zullen je zo goed als mogelijk informeren.

Bespreek dit in jullie groep en evalueer samen of de verwachte impact de risico's waard is en of iedereen zich er comfortabel bij voelt.

C'EST PAAAARTI...

Consensus d'action
Discutez de la nécessité au sein de votre groupe d'établir un cadre d'action et convenez de la portée que vous souhaitez donner à l'action (ce qui vous semble acceptable et ce qui ne l'est pas).

Lisez également le consensus d'action de Stop Arming Israel Belgium et discutez-en pour savoir si vous êtes d'accord avec celui-ci.

Préparation pratique

- Consultez la liste des noms d'avocat.es fiables et complétez-la éventuellement avec les noms d'avocat.es actif.ves dans la province/région du lieu de l'action. Il doit s'agir d'avocat.es spécialisé.es en droit pénal.
- Décidez de la manière dont les activistes peuvent vous contacter. Gardez à l'esprit que cela doit être possible depuis le commissariat de police. Il est fortement recommandé d'utiliser un numéro anonyme enregistré sur un téléphone propre et fonctionnant depuis un endroit anonyme. Vous pouvez également convenir qu'en cas d'arrestation, les activistes contactent un.e membre de leur famille ou un.e ami.e qui n'est pas impliqué.e dans l'action et qui contactera ensuite votre équipe juridique via Signal.
- Choisissez un lieu à partir duquel l'équipe juridique suivra l'action. N'oubliez pas que si vous souhaitez être joignable par téléphone, vous devez choisir un lieu accessible au public afin que personne ne puisse être incriminé.e à la suite d'une enquête sur les données téléphoniques (connexion à l'antenne relais).

Informations et accords avec les activistes

- Dressez une liste de toutes les personnes qui risquent d'être arrêtées. Veillez à le faire pour tout le monde, y compris les éclaireur.ses ou les personnes qui apportent simplement du matériel ou conduisent des activistes.
- Recueillez les informations suivantes :
  - Qui contacter en cas d'arrestation si quelque chose tourne mal, après combien de temps et avec quel message (par exemple : après 24 heures, appeler la sœur pour prévenir son travail, appeler les colocataires).
  - Informations médicales importantes (par exemple : ne peut pas passer 24 heures sans médicaments psychotropes).
  - Informations sur d'autres procédures judiciaires (procédure de séjour, etc.) et avocat.es.
- Convenez clairement des lieux où les gens se retrouveront et de la manière dont l'équipe juridique sera tenue informée.

Encouragez les activistes à choisir un « nid » ou un lieu de rendez-vous clair où les gens pourront se retrouver s'ils se perdent de vue ou s'ils sont libéré.es pendant la nuit. Convenez de la durée du séjour à cet endroit et du moment où vous vous déplacerez vers un autre lieu.

Anticiper les lieux d'arrestation
En fonction du lieu de l'action, vous pouvez déjà anticiper où les personnes seront éventuellement emmenées en cas d'arrestation. Connaissez-vous des personnes qui habitent dans les environs où les activistes peuvent se rendre s'ils sont libéré.es ?

2. Comment rejoindre et quitter le site sans se faire détecter

Le transport est une partie importante de n'importe quel plan et peut faire la différence entre s'en sortir et se faire arrêter. Voici quelques exemples de différents modes de transport et de comment vous pourriez les utiliser à votre avantage:

- Marcher jusqu'à la cible peut être très efficace. La clé est de garder votre visage masqué tout du long et de trouver un endroit pour changer vos vêtements et continuer votre chemin. Essayez de trouver un lieu avec du monde pour vous changer, comme un centre commercial, ou un lieu avec plusieurs sorties comme un parc afin de ne pas pouvoir être facilement traqué.es par les caméras.
- A vélo. Les vélos sont super pour les actions discrètes. Garez vos vélos proche de votre cible à un endroit sans caméras. Puis marchez à partir de là pour faire votre action et revenez prendre vos vélos pour partir. Assurez-vous que vos vélos ne soient pas facilement reconnaissables et, si nécessaire, empruntez un vélo neutre pour que vous n'aiyez pas à utiliser votre vélo personnel recouvert de stickers militants.
- Une voiture est parfois le meilleur moyen de se déplacer. Mais elles ont des numéros d'immatriculation qui peuvent être relevés par des caméras et permettre d'identifer le.a propriétaire. Si vous prévoyez d'utiliser une voiture faites en sorte d'avoir repéré toutes les caméras qui se trouveront sur votre route, et idéallement trouvez un moyen de les contourner. Ne vous garez pas proche du lieu de l'action, mais à un endroit sans caméras.
- Si vous utilisez les transports en commun, n'utilisez pas votre propre carte bancaire ou carte Mobib. Cette information est stockée et peut facilement être utilisée par la police. Il est toujours préférable d'utiliser du liquide. Toutefois, de nos jours beaucoup de transports en commun n'acceptent pas les paiements en liquide. Si vous être sur Bruxelles, il vaut mieux utiliser une carte Mobib anonyme que vous avez rechargée avec du cash. Gardez en tête que les transports en commun sont truffés de caméras, donc gardez votre visage couvert. Cepedant, entrer dans un bus ou un train avec une cagoule peut sembler suspect. Pensez à d'autres moyens de recouvrir votre visage, les masques chirurgicaux, par exemple, sont devenus courant depuis le COVID, vous pouvez aussi mettre des lunettes de soleil.

Le trajet. Lorsque vous choisissez votre mode de transport, assurez-vous d'avoir considéré précautionneusement toutes les routes afin de vous assurer une fuite parfaite. Pensez aux positions des caméras et n'otez pas votre masque trop tôt. Si la police veut vous trouver, elle vous suivra grâce aux caméras jusqu'à l'endroit où vous aurez retiré votre masque et obtiendra une image de votre visage. Porter une casquette peut aider à masquer votre visage mais sans garantie. Il vaut mieux rester couvert jusqu'à un endroit sûr, sans caméras et relativement peuplé. A partir de là vous prévoir votre trajet jusqu'à chez vous.

3. RÔLES

Si plus d'une personne est impliquée dans l'action, vous devez vous répartir les rôles. Par exemple si vous voulez qu'une personne se concentre exclusivement sur la prise de photos et vidéos, alors cette personne doit se concentrer là-dessus et pas sur le fait d'agiter des marteaux ! Les autres peuvent se disperser dans différentes zones du site, ou une personne peut usage de peinture et un autre avec quelque chose d'autre 😉

Peu importe la forme de votre action, assurez-vous de bien savoir qui fait quoi pour être aussi efficaces et rapides que possible. C'est pour ça qu'il faut absolument bien plannifier votre action, de sorte à ce que chacun.e sache exactement ce qu'iel doit faire.

Soutien extérieur - faites en sorte qu'une ou deux personnes qui ne participent pas à l'action soient au courant de vos plans. Vous devrez contacter cette personne lorsque vous arriverez sain.es et sauf.ves chez vous. Cette personne n'a pas besoin de connaître tous les détails, mais doit avoir des consignes pour le cas où vous vous feriez arrêter (appeler un.e avocat.e, nourir votre chat, appeler votre travail pour dire que vous êtes malade etc). Assurez-vous que cette personne ait toutes les informations nécessaires, dont le nom et numéro de téléphone d'un.e avocat.e.

3. L'ÉQUIPEMENT

Maintenant que votre plan est prêt dans les moindres détails, il est temps d'acheter l'équipement nécessaire. C'est le bon moment pour vous rappeler que LE LIQUIDE EST ROI. Lorsque vous achetez du matériel, que ce soit des bombes de peinture ou des masses, ne laissez aucun papiers ou traces numériques trainer. Utilisez du cash et portez une casquette ou un masque COVID par précaution. Ne vous comportez pas de manière suspecte. Vous pouvez aussi demander à un.e ami.e qui ne participera pas à l'action de faire les achats pour vous. Et vous pouvez acheter différents équipements dans différents magasins.

Le matériel dont vous aurez besoin va dépendre de votre action. Elle peut demander des bombes de peintures, des extincteurs remplis de peinture,... N'oubliez pas de porter des gants et lunettes de protection: vous ne voulez pas vous coupez et laisser vos empreintes digitales ou votre sang sur place !

Si vous avez besoin de conseil sur le matériel, par exemple pour remplir un extincteur de peinture, contactez-nous par e-mail: contact@stop-arming-israel-belgium.com où via Signal si vous avez déjà un contact direct.

Important: ne laissez aucun objet derrière vous après votre action. Absolument rien si ce n'est de la peinture et de la destruction. La police pourrait décider de lancer des investigations forensiques sur les objets que vous laissez dans le but de retracer vos identités.

4. LES HABITS

- Le plus important est de se masquer le visage. Votre visage ne doit jamais être visible durant l'action. Une cagoule est le mieux pour ça, mais vous pouvez aussi utiliser une casquette, un masque chirurgical et des lunettes de soleil. Si vous portez des lunettes de vue essayez de trouver une meilleure solution (lentilles, de vielles lunettes, pas de lunettes).
- Portez des chaussures "normales" qui ne sortent pas du lot. Ne portez pas des chaussures avec lesquelles vous vous êtes déjà fait.es arrêté.es lors d'une précédente action ou manifestation, ou que vous portez sur des photos trouvables sur les réseaux sociaux. Il vaut mieux acheter les chaussures noires les plus ordinaires et ennuyeuses possibles et de ne les porter que pendant l'action.
- Portez des vêtements sombres (de préférence noirs) qui n'attirent pas l'attention. Portez des vêtements amples, cela rend plus difficile d'estimer votre carrure.
- Couvrez la totalité de votre corps. C'est particulièrement important si vous avez des signes distinctifs tels que des tatouages ou des grains de beauté. Portez des gants comme mentionné plus tôt et assurez-vous que tout soit couvert.
- Portez des vêtements que vous êtes prêt.es à jeter après l'action.

ETAPE 5 - L'ACTION

L'adrenaline va traverser votre corps et vos nerfs seront mis à rude épreuve par la même occasion. C'est normal. Repasser au travers de vos plans avant de passer à l'action afin de vous assurer que tout est clair pour tout le monde.

Supprimez Signal de votre téléphone et ordinateur pour ne pas laisser de traces au cas où votre maison serait perquisitionnée par la suite. Déconnectez votre ordinateur de tous les outils que vous avez pu utiliser durant la préparation de l'action. Et jetez toutes les preuves physiques comme des papiers avec des notes.

Allez-y ! C'est le jour j, vous avez bien plannifié votre action, vous êtes reposé.es et prêt.es. Bonne chance !

1. DOCUMENTER VOTRE ACTION

Le but principal de votre action doit être de causer des dégats économiques et d'exercer de la pression sur l'entreprise. Toutefois, ne sous-estimez pas le potentiel de la communication afin que le message puisse se transmettre d'autant plus largement. De cette manière, d'autres cibles potentielles pourront voir ce qui les attends, cela peut inspirer d'autres groupes à passer à l'action et, encore plus important, les personnes en Palestine sauront que notre solidarité est crystallisée par des actions.

Quelques éléments utiles :

- Téléchargez un logo de notre campagne sur notre site web.
- Renseignez-vous sur Elbit et les autres campagnes qui les cible sur notre site web.
- Logiciels gratuits pour éditer des vidéos et/ou des images: Canva (en ligne), inkscape (hors ligne), Gimp (hors ligne), Premiere pro (hors ligne). Si vous travaillez en ligne, faites toujours attention à suivre les bon comportements de sécurité numérique. Soyez vigilant.es avec les les logiciels hors ligne qui peuvent automatiquement sauvegarder en ligne des données.

Sécurité numérique

- Lisez attentivement les consignes de sécurité numérique à la fin de ce manuel.
- Ne prenez JAMAIS votre propre téléphone en action car il peut être utilisé pour vous identifier. Idéallement, donnez votre téléphone à un.e ami.e qui l'emmenera en promenade dans des lieux sans caméras (comme des parcs) pour que vous puissiez créer des preuves du fait qu vous n'étiez pas sur les lieux de l'action.
- Pour documenter votre action via des photos et vidéos, achetez un smartphone bon marché. Payez avec du liquide. Pour plus d'informations sur l'utilisation sécurisée de ce téléphone jetable, consultez les consignes de sécurité numérique à la fin de ce document.
- Lorsque vous filmez ou prenez des photos, assurez-vous que personne ne soit identifiable. Coupez les segments où des personnes sont identifiables ou envoyer des instrucctions claires pour l'édition.

Ecrire un communiqué de presse

- Commencez par un court résumé des détails essentiels dans le premier paragraph en répondant aux 5 points: qui, quoi, quand, où et pourquoi ?
- Soyez concis.es: votre communiqué doit rester court.
- Soyez pertinent.es: expliquez à votre audience pourquoi elle doit y accorder de l'importance.
- Structurez-le: utilisez des titres clairs pour introduire les paragraphes afin d'aider les journalistes à lire le texte rapidement.
- Décrivez votre action objectivement et mettez les parties politiques, "subjectives" entre guillemets. Par exemple: X a dit, "Cette entreprise est complice de génocide" (cela permettra aux journalistes de publier le texte tel quel).
- Incluez un paragraphe sur le contexte général de la campagne et/ou sur l'entreprise afin de situer votre action pour les journalistes.
- Envoyez-nous votre communiqué de presse, ou envoyez-le vous-même avec une adresse mail sécurisée si vous avez déjà une liste de presse à contacter !

Réseaux sociaux

- Vous pouvez nous envoyer de quoi poster sur nos réseaux sociaux. Nous pouvons aussi collaborer sur des publications si vous voulez utliser votre propre compte.
- Les publications qui fonctionnent le mieux sont des courtes vidéos (2-3 min). Essayez de commencer avec les images les plus impressionantes pour capter l'attention. La musique peut être ajoutée à la publication directement via Instagram.
- Sinon, préparez une série d'images pour la publication d'un caroussel avec un texte explicatif.
- S'il vous plait envoyez-nous la légende pour vos photos/vidéos, préférablement en néerlandais et français. Nous réservons en général l'anglais pour les publications principales.

Nous envoyer vos matériaux

S'il vous plait lisez le consensus d'action pour savoir ce que nous acceptons et n'acceptons pas de publier sur nos réseaux sociaux et site web.

Effacez les métadonnées de vos fichiers avant de la envoyer. Il s'agit de toutes les données qui pourrait contenir des informations permettant de vous identifier. Nettoyez les fichiers sur votre ordinateur (crypté) à l'aide de Metadata Cleaner (https://metadata.systemli.org/).

Pour envoyer votre communiqué de presse, photos et vidéos de manière sécurisée, nous vous recommandons de créer un dossier sur un cryptdrive anonyme en utilisant un VPN + TOR. Vous pouvez créer un cryptdrive ici: https://cryptpad.fr/

Vous pouvez ensuite envoyer le lien vers ce dossier via une adresse mail Proton anonyme (avec un VPN) à notre adresse Proton: stop-arming-israel-belgium@proton.me (les mails entre deux adresses Proton sont cryptés).

2. ET SI LES CHOSES SE PASSENT MAL ?

Vous assurez la permanence et le soutien pendant l'action pour vos camarades. Cela signifie que vous faites un suivi de l'action et des éventuelles arrestations qui en découlent et que vous apportez, dans la mesure du possible, un soutien physique et émotionnel.

Suivre le temps d'arrestation :

- Notez l'heure à laquelle tes camarades ont été arrêté.es si tu disposes de cette information.
- Veillez à ce qu'ils ne soient pas détenus trop longtemps.

Suivi pendant les premières 24 à 48 heures :

Tant que la personne arrêtée est en détention administrative ou n'a pas encore été interrogée dans le cas d'une détention judiciaire, le plus important est le soutien et les soins. D'un point de vue juridique, il n'y a pas grand-chose à faire à ce stade. Tant qu'il n'y a pas eu d'interrogatoire, aucun.e avocat.e n'est officiellement désigné.e. Il ne peut donc rien faire à ce stade.
En cas de détention judiciaire, un interrogatoire peut avoir lieu. À ce moment-là, les personnes arrêtées peuvent communiquer le nom d'un.e avocat.e que la police doit contacter. C'est à ce moment-là qu'il peut être utile de contacter l'avocat.e (si vous savez lequel a été désigné). L'avocat.e peut vous informer du statut de l'arrestation, du lieu de détention, etc.

- Appelez les personnes à contacter si cela a été convenu.
- Appelez éventuellement les commissariats de police (ou l'hôpital) si vous ne disposez d'aucune information sur le lieu où se trouvent les personnes arrêtées. Réfléchissez bien au numéro avec lequel vous appelez. Il peut être plus sûr de demander à une personne proche des personnes concernées et qui n'est pas impliquée dans l'action de passer l'appel. Respectez les accords conclus avec les activistes. Les avocat.es ne peuvent pas vous aider dans ce cas, car la personne n'est pas encore officiellement leur client.e.

Suivi en cas d'arrestation prolongée

Si une personne est détenue pendant plus de 48 heures ou après avoir été entendue par un juge d'instruction, il y a de fortes chances que le juge d'instruction ait délivré un mandat d'arrêt. Cela signifie que la personne peut être détenue plus longtemps et sera transférée en prison.

Dans le cas ou la personne à choisie de rester anonyme, il est également possible qu'elle soit transférée vers un centre fermé sous prétexte qu'elle n'a pas de papiers.

- Prenez contact avec l'équipe juridique de Stop Arming Israel Belgium.
- Cherchez un.e avocat.e qui pourra assurer le suivi.
- Vérifiez avec l'avocat.e s'il peut être utile de communiquer sur les reseaux sociaux sur la situation.
- Envisagez d'organiser des manifestations devant le commissariat/la prison/le centre fermé.
- S'il s'agit d'une personne envoyée dans un centre fermé et si cette personne n'a pas la nationalité belge, il est important de contacter l'avocat.e qui suit la procédure de séjour.

Suivi / Soutien aux personnes arrêtées :

- Rendez-vous au poste de police ou au lieu de rendez-vous convenu. Il est vraiment très utile que des personnes attendent les personnes arrêtées à leur sortie du poste de police. Souvent, les personnes n'ont pas de téléphone et ont besoin de parler à quelqu'un.e. Le fait que quelqu'un.e les attende peut faire une grande différence.
- Apportez du café, du thé ou des biscuits (ou autre chose).
- Écoutez la personne / Soyez disponible / Faites quelque chose d'agréable.

ETAPE 6 - APRÈS L'ACTION

1. EFFACER SES TRACES

Vous venez de perturber une entreprise complice de génocide. Vous voulez maintenant vous débarasser de toutes les preuves. S'il vous reste des bombes de peintures vides ou d'autres objets, débarassez(vous en le plus tôt possibl, après les avoir nettoyés au cas où vous les auriez touchés sans gants.

- Ne les jetez pas dans la poubelle de votre maison, trouvez plutôt un lieu public pour le faire. Si vous ne voulez pas jeter vos vêtements, faites en sorte qu'ils ne soient pas chez vous ou dans votre voiture. Amenez-les chez un.e ami.e.
- Tout cela peut sembler excessif, mais il est très rassurant de savoir qu'aucune preuve ne reste sur le lieu de l'action ou chez vous. Si la police finit par perquisitionner votre domicile (ce qui est très peu probable si vous suivez toutes les étapes plus haut), elle cherchera des objets permettant de vous lier à l'action.

N'oublier pas de:

- Envoyer vos photos et vidéo à la campagne Stop Arming Israel Belgium : contact@stop-arming-israel-belgium.com
- Supprimer toutes les photos sur le téléphone d'action.
- Retirer toutes les métadonnées sur les fichiers compromettants.
- Editer tout ce qui pourrait révéler votre identité sur les photos/videos (voix, visages etc).

En plus des photos et vidéos, vous pouvez aussi nous envoyer votre communiqué de presse que nous transférerons à des journalistes en plus de votre campagne.

2. SURVEILLER LES CONSÉQUENCES JURIDIQUES.

Assurez le suivi juridique et surveillez la répression.

- Envoyez à l'équipe de soutien juridique un petit compte-rendu de ce qui s'est passé.
- Après l'action, vous pouvez aider vos camarades en les accompagnant et en les soutenant dans les démarches juridiques.
- Contactez l'équipe de soutien juridique pour vous aider dans d'éventuelles procédures judiciaires.

SÉCURITÉ NUMÉRIQUE

Avant-propos :
Ce manuel a pour but d'initier aux bonnes pratiques de sécurité numérique, sans rentrer dans des détails technique mais. Pour des guides plus rigoureux et complets:

- https://technopolice.be/autodefense-numerique/
- https://guide.boum.org/
- https://zadducarnet.org/index.php/2021/01/10/guide-de-survie/

1. PRÉCAUTIONS DE BASE

TOUTE activité sur un objet électronique laisse des traces qui peuvent être exploitées par des personnes compétentes.

Conseil numéro 1: Eviter toute action qui n'est pas nécessaire. Exemple: ne télécharge pas des fichiers depuis un cloud, même si tu n'aimes pas l'éditeur en ligne, car il laissera des traces sur ton appareil.

Conseil numéro 2: prends toujours des précautions. Utilise un blaze dans la vie réelle et des faux noms sur internet. Ne mets pas toutes tes informations au même endroit, ne lie pas tes comptes, tes données et tes espaces entre eux.

Conseil numéro 3: Ne va pas trop vite. Ces conseils de base doivent toujours être suivis, tu pourras utiliser des outils techniques par la suite mais ceux-ci ne doivent jamais remplacer les principes de sécurité de base.

Conseil numéro 4: La sécurité est collective. Si dans un groupe une personne prend la sécurité à la légère, cette personne peut servir de point d'accès et compromettre la sécurité de tout le groupe.

Lors d'une réunion
Ne pas parler d'actions sensibles à des personnes qui n'ont pas besoin d'être au courant.
Rassembler les téléphones et les mettre à l'écart dans une autre pièce.

Si besoin d'un ordinateur, privilégier un ordinateur crypté et, s'il est nécessaire de se connecter à internet, utiliser un VPN et TOR (explication détaillée ci-dessous).

Demander à tout le monde d'avoir activé son mode avion bien avant d'arriver (à quelques kms du lieu), cela évitera que les opérateur téléphoniques puissent prouver que vous étiez toustes ensemble (bornage et géolocalisation collective).
Changer de lieu à chaque réunion.

Hors réunions
Si des personnes n'ont pas besoin de savoir, ne leur dites rien. Ne dites pas que vous êtes dans l'organisation de telle ou telle action. Cela vaut aussi pour les membre de votre familles ou ami.es proches.

S'il s'agit de camarades qui ont besoin d'informations sur l'action, donne leur uniquement ce qu'iels ont besoin de savoir pour leur rôle.

Si tu dois te déplacer pour des activités sensibles comme un reperage, active le mode avion. Idéalement, active-le régulièrement de manière aléatoire pour des durées aléatoire afin de brouiller les pistes.

2. ORDINATEUR

Eviter au maximum d'utiliser son téléphone pour des recherches en en rapport avec une action (maps, repérages de lieu, infos sur internet...). Fais tes recherches sur ordinateur en utilisant un VPN+TOR.

Autant que possible, ne sauvegarde pas de documents sensibles. Chiffre ton ordinateur. Le mot de passe utilisateur ne protège pas grand chose.

Supprimer un document sur un ordinateur ou une clé ne le supprime pas vraiment et il est possible de le récupérer. Pour supprimer un fichier sur un disque (disque dur, clé USB, carte SD...) il faut écraser les données et le formater.

Chiffrement
Chiffrer, ou crypter des données, c'est les transformer de sorte à ce qu'elles ne soient lisible que par des personnes autorisées à le faire. Pour accéder au contenu d'un disque crypté, il faut posséder la "clé", par example un mot de passe.
Il y a deux précautions principales à prendre en compte:

- L'ordinateur n'est chiffré que lorsqu'il est éteint, alors éteins-le, ne le laisse pas simplement en veille
- La force du chiffrement dépend de la force du mot de passe choisi, alors fais en sorte qu'il soit long (20+ caractères) et idéalement un mix aléatoire de lettres minuscules, majuscules, chiffres et symboles spéciaux.

Comment chiffrer son ordinateur

Il vaut mieux éviter d'utiliser le programme de chiffrement natif fourni avec ton ordinateur, par exemple l'option de chiffrement via BitLocker de Windows. On n'a pas spécialement envie de faire confiance à Microsoft. Voici nos recommandations:

- Pour un ordinateur sous Linux, il est possible de crypter le disque à l'installation de Linux via la spécification LUKS. Plus de détails pour Ubuntu par exemple: https://documentation.ubuntu.com/security/security-features/storage/encryption-full-disk/
- Pour Windows le chiffrement se fera après l'installation. Cette méthode est aussi applicable à Linux. Nous recommandons VeraCrypt, ici le guide du débutant: https://veracrypt.io/en/Beginner%27s%20Tutorial.html.

Mots de passes

Un bon mot de passe est constitué de mots/caractères aléatoires, incluant des minuscules, majuscules, symboles et chiffres. Idéalement, vise un minimum de 15 caractères.
Gestionnaire de mot de passe: Un gestionnaire de mot de passe peut générer des mots de passe forts et mémoriser tes mots de passe. Le côté pratique est que tu n'as qu'un seul mot de passe à retenir. Le contre-coup est que si ce mot de passe est cracké par une personne, celle-ci a alors accès à la totalité de tes mots de passes stockés. De bon gestionnaires sont Keepassxc et bitwarden. Mieux vaut ne pas utiliser le gestionnaire natif (proposé par ta machine par défaut).

3. DOCUMENTS ET CLOUDS

Créer un drive commun sur https://cryptpad.fr/, il suffit de se connecter pour accéder au drive.

Ce drive doit être TOP SECRET. Il ne faut pas l'envoyer à n'importe qui, uniquement des personnes safes liées à l'organisation. Il ne faut pas non plus mettre tout et n'importe quoi dessus.

Nettoyer régulièrement ce drive pour ne pas laisser trainer des fichiers compromettants qui ne sont plus nécessaires.

- Toujours accéder au drive en utilisant un VPN+TOR.
- Ne jamais accéder au drive sur téléphone!
- Attention: si tu veux partager un cryptpad ou un fichier, il faut cliquer sur partager et non copier-coller l'URL de la page.
- Optionnel: il est possible de programmer la destruction d'un cryptpad ou de fichiers. Si la destruction n'est pas programmée: supprimer le pad après l'action, ou lorsqu'il n'est plus nécessaire.
- Ne pas mettre de nom/lieu/date/infos perso sur le pad.

4. SIGNAL

Signal, avec son chiffrement de bout-en-bout, est une très bonne messagerie. Mais si la police met la main sur ton téléphone, elle pourra avoir accès à tes conversations et aux profils de tes camarades. Chaque profil étant lié à un numéro de téléphone et donc à une carte d'identité, tout le groupe est alors identifié. Voici quelques conseils pour éviter cela:

Sur le plan individuel

Active le verrouillage de l'écran pour Signal. Sur ton compte:

- paramètres > confidentialité > verrouillage de l'écran > "activer le verrouillage de l'écran".
- Définir le temps de verrouillage à quelques minutes
- Il est donc important d'avoir un PIN ou mot de passe fort sur ton téléphone car Signal utilise la meme PIN. Plus le mot de passe est long et aléatoire, mieux c'est.

Masque ton numéro de téléphone. Sur ton compte:

- paramètres > confidentialité > numéro de téléphone > "qui peut voir mon numéro de téléphone" > personne
- paramètres > confidentialité > numéro de téléphone > "qui peut me trouver grâce à mon numéro de téléphone" > personne

Active les messages éphémères par défaut, afin qu'ils s'appliquent à toute nouvelle conversation que tu lances:

- paramètres > confidentialité > messages éphémères > choisissez la durée de votre choix
- Les messages de ces conversations seront ainsi supprimés au bout de cette durée. Plus la durée est courte plus la sécurité est élevée, mais plus cela peut-être contraignant.

Tu peux modifier à tout moment les messages éphémères dans une conversation déjà existante en suivant:

- Sur la conversation: en haut à droite > paramètres de la conversation > messages éphémères > choisir la durée de votre choix
- Attention, cette modification n'est pas rétroactive, les messages envoyés avant la modification garderont leur temps de vie initial

Sur le plan général

Créer un nouveau groupe tous les 6 mois et ne donner le lien qu'en personne ou via des contacts connus et safe. Quitter et supprimer l'ancien groupe.

Ne pas parler des action privées / sous-groupes dans un grouper plus général si ce n'est pas nécéssaire.

Avant d'ajouter une personne sur signal, assurez-vous qu'elle a les connaissance de base en sécurité, en ayant lu ce manuel par exemple.

Vérifie la liste des membres des groupes de temps en temps et si un pseudo ne te dit rien, demande à tes camarades de qui il s'agit. Si personne ne sait, ou que la personne est inactive depuis longtemps, retirez-la du groupe en lui expliquant qu'elle peut toujours vous contacter si elle compte se ré-investir.

Après ou juste avant l'action, quitter et supprimer le groupe.

5. EMAIL

Adresses e-mail safe:

- Protonmail (https://proton.me/mail)
- Riseup (https://riseup.net/en/email/settings/mail-accounts)
- Autres mails: systemli.org ; autistici.org ; immerda.ch

Attention, les échanges ne sont chiffrés automatique qu'entre les mêmes hébergeurs (c'est à dire d'une adresse proton à une autre adresse proton par exemple). Pour chiffrer un mail entre deux fournisseurs différents, il faut une clé publique de chiffrement / open PGP (= chiffrement asymétrique) :

PGP avec Protonmail
Avec des adresses protonmail il est facile de générer une clé publique de chiffrement, à communiquer à ton ou ta correspondant.e.

Sur proton : nouveau message > ... (en bas) > joindre une clé publique (plus d'infos https://proton.me/support/how-to-use-pgp)

Il est moins facile pour ton ou ta correspondant.e de l'intégrer à son mail si elle n'a pas l'une des adresses mentionnées ci-dessus.

VPN
Un VPN (Virtual Private Network, ou réseau privé virtuel) est un service qui crée une connexion sécurisée et chiffrée entre votre appareil et Internet. Concrètement, il fait transiter vos données par un serveur intermédiaire, ce qui masque votre adresse IP réelle et protège votre activité en ligne. Grâce au chiffrement, les informations que vous envoyez et recevez deviennent illisibles pour des tiers.

Gratuits et fiables : Proton VPN https://protonvpn.com/ ou riseup VPN https://riseup.net/en/vpn.

Payants et fiables : Mullvad https://mullvad.net/en
Proscrire l'utilisation d'autres VPN, tels que Nord VPN qui ne sont pas sécurisés voir pire, sont des facteurs de risques conséquent qui peuvent récolter des données.
Un VPN ne suffit pas pour faire des recherches de manière sécurisée (voir TOR).

6. TOR

The Onion Router ou TOR désigne à la fois un réseau internet, un protocole de chiffrement et un navigateur internet. De manière générale, lorsque l'on parle de TOR, il s'agit du navigateur inter. Ce navigateur fait transiter les données des recherches par le réseau TOR et applique son protocole de chiffrement afin de les protéger.

Du fait de toutes ces mesures, la connexion peut être lente voire être rompue par moment, certains sites peuvent être mal affichés tandis que d'autres peuvent décider de bloquer les connexion via TOR.

Tu trouveras plus d'informations sur le site du projet TOR: https://support.torproject.org/about-tor/.

Pour télécharger et installer le navigateur TOR c'est très simple, tu n'as qu'a te rendre ici: https://www.torproject.org/download/. Il existe également d'autres navigateurs qui intègrent Tor, comme Brave.

Attention: TOR n'est pas tout-puissant, il ne fait que rendre plus difficile de te tracer ou t'identifier en ligne. Utiliser TOR ne doit pas te faire oublier les pratiques de sécurité de base.

7. TÉLÉPHONES D'ACTION

Si vous devez emporter un téléphone avec vous lors d'une action, par exemple pour prendre des photos et des vidéos, assurez-vous que ce téléphone n'est pas lié à votre identité :

- Achetez un téléphone « vierge », qui peut être d'occasion, mais pas un ancien téléphone que vous, vos amis ou les membres de votre famille avez utilisé auparavant. Rendez-vous dans un magasin de téléphonie et payez en espèces.
- Utilisez une carte SIM anonyme. Pour cela, vous devrez vous rendre aux Pays-Bas.

Pour la carte SIM néerlandaise, veillez à activer la carte SIM et l'internet mobile aux Pays-Bas dans un téléphone « vierge ». Ce n'est qu'alors que le téléphone fonctionnera en Belgique. Veillez à acheter un crédit d'appel supplémentaire aux Pays-Bas, car le crédit que vous pouvez acheter en Belgique ne fonctionne pas avec les cartes SIM néerlandaises. Lebara fonctionne le mieux. Payez tout en espèces.

N'allumez jamais ce téléphone d'action chez vous ou dans tout autre endroit qui vous est lié, et ne le connectez pas au Wi-Fi à la maison ou au travail sans VPN. De plus, si vous sortez pour l'utiliser, laissez votre propre téléphone à la maison ou mettez-le à l'avance en mode avion. N'utilisez pas un téléphone que vous avez déjà utilisé pour d'autres actions.