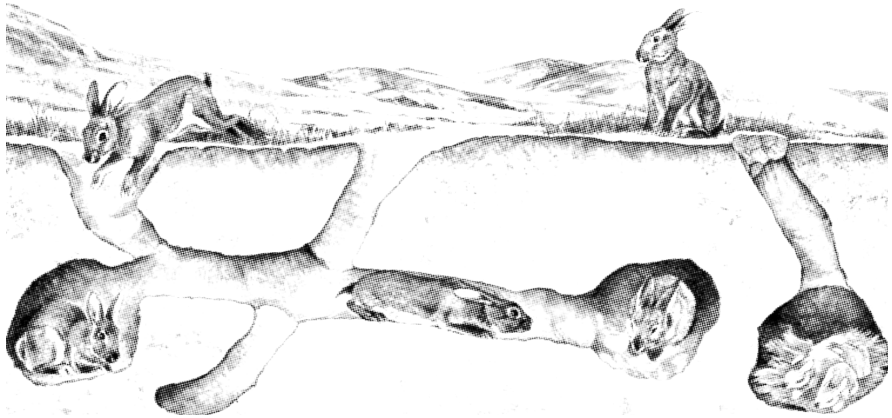
“[Je] veux avoir le genre de pratiques sécuritaires qui me permettent d’être ouverte tout en sachant que j’ai évalué les risques auxquels je suis exposée et que je prends des mesures intelligentes pour les minimiser. La culture de sécurité devrait rendre l’ouverture plus possible, pas moins. Cette proposition de culture de la sécurité repose sur un recadrage – sur le passage de la peur à la confiance, de l’aversion au risque au courage, de l’isolement à la connexion, et de la suspicion à la confiance.”

Mise en page par le Centre de documentation sur la contre-surveillance (csrc.link)

Assurance, courage, lien, confiance : une proposition de culture de sécurité

2019



Quand on parle de culture de sécurité, les gens vivent généralement l'une de ces deux expériences : la première est de construire des murs et de tenir les autres à l'écart, la seconde est d'être soi-même exclu et de ne pas avoir la confiance des gens. Dans les deux cas, il y a des sentiments négatifs – la peur et la suspicion pour le premier et un sentiment d'aliénation et du ressentiment pour le second. Je dirais que ce sont les deux côtés d'une même médaille, deux expériences d'une culture de sécurité qui ne fonctionne pas bien.

Je veux être accueillante et ouverte aux nouvelles personnes quand je m'organise. Je veux aussi me protéger du mieux possible des efforts visant à perturber cette organisation, surtout de la part de l'État, mais aussi des patrons ou de l'extrême droite. Cela signifie que je veux avoir le genre de pratiques sécuritaires qui me permettent d'être ouverte tout en sachant que j'ai évalué les risques auxquels je suis exposée et que je prends des mesures intelligentes pour les minimiser. La culture de sécurité devrait rendre l'ouverture plus possible, pas moins.

Cette proposition de culture de la sécurité repose sur un recadrage – sur le passage de la peur à la confiance, de l'aversion au risque au courage, de l'isolement à la connexion, et de la suspicion à la confiance.

Il est logique d'avoir peur – l'État est très puissant, la répression est fréquente et elle a le pouvoir de nous écraser, nous et tous nos projets. Mais je ne veux pas rester coincée avec cette peur. Avec des informations précises et un bon plan, nous pouvons commencer à transformer la peur en confiance, sachant que nous avons des pratiques de sécurité à la hauteur du risque auquel nous faisons face. En fait, sans transformer la peur, il est difficile d'imaginer comment même agir face au pouvoir de nos ennemis.

Je ne veux pas avoir peur du risque. Je veux faire le choix de mes actes en fonction de leur efficacité, de leur pertinence, de mon analyse et de mon éthique. Une bonne culture de sécurité nous permet de faire preuve de courage dans nos tactiques collectives, car nous savons que nous pouvons gérer le risque. Lorsque nous ne transformons pas l'aversion au risque, nous nous autopoliçons et restons confinés à l'espace d'opposition symbolique qui nous est fourni.

La répression fonctionne en isolant les gens. Je ne veux pas contribuer à cet isolement par ce que je fais pour ma sécurité et celle de mes ami.e.s. Je veux une culture de sécurité enracinée dans l'approfondissement de nos connexions les un.e.s avec les autres. Quand nous ne dépassons pas l'isolement, l'organisation risque de ressembler au travail et de ne pas permettre le genre de relations qui nous transforment vraiment, de façon à pouvoir ressentir le monde que nous voulons créer.

Je ne veux pas me méfier des gens que je rencontre. C'est toxique et désagrège les espaces de lutte que nous créons. Plutôt que de ressentir de la méfiance envers quelqu'un, je préfère me demander : «Qu'est-ce que ça prendrait pour que je fasse confiance à cette personne ? » Je veux aller vers les gens et essayer de transformer la méfiance en confiance.

Je voudrais proposer une définition de culture de sécurité pour donner une perspective à cette conversation. La culture de sécurité fait référence à un ensemble de pratiques développées pour évaluer les risques, pour contrôler les flux d'informations dans nos réseaux et pour construire des relations fortes pour la lutte. Il existe d'innombrables cultures de sécurité possibles, mais la chose la plus importante est qu'elles viennent de discussions claires et explicites à propos du risque et répondent au changement. Dans l'exemple qui suit, la conversation en cours sur le risque répond aux modifications de nos actions et à comment nous sommes ciblés. Les pratiques variées de cultures de sécurité mentionnées seront expliquées plus loin.

Dans une campagne contre un oléoduc, là où je vis, nous avons voulu mettre l'accent sur les actions directes de masse visant les infrastructures pétrolières. Nous avons décidé que, pour les premières étapes de cette campagne où nous nous concentrions sur la sensibilisation et la recherche, le risque que nous courions était très faible et que nous pouvions en toute sécurité faire participer de nombreuses personnes à ces travaux, et partager ouvertement l'information à ce sujet sur n'importe quelle plateforme. Lorsque nous avons commencé à planifier des actions de protestation symboliques, cette considération n'a pas beaucoup changé, mais lorsque nous avons commencé à planifier des choses comme le blocage de routes ou le piquetage d'un

poste de police, l'élément de surprise est devenu une considération plus importante. Peu importe les accusations criminelles possibles, nos actions seraient tout simplement moins efficaces si elles étaient connues à l'avance. Nous avons donc cessé d'utiliser des moyens de communication publics ou facilement surveillés et avons commencé à demander que les gens ne communiquent les détails qu'à des personnes de confiance ayant l'intention de participer.

Peu après le début de cette phase de la campagne, un dispositif policier national appelé Joint Intelligence Group (JIG) s'est réuni pour défendre les oléoducs, avec la participation de plusieurs niveaux de police et de services de renseignement. Les JIG et les configurations de ce genre constituent une menace spécifique aux luttes de toutes sortes, car ils visent directement à perturber l'organisation grâce à de vastes ressources. Donc, même si nos actions n'ont pas changé, nous avons r et avons décidé d'isoler les organisateurs des actions de possibles accusations de conspiration en faisant la planification dans un petit groupe opaque. Nous pourrions inviter à participer des personnes en qui nous avons confiance, et nous pourrions prendre des mesures pour établir cette confiance, comme faire des vérifications d'identité les uns des autres. Mais nous ne planifierions plus les actions ouvertement dans le cadre du réseau plus large de personnes intéressées par le travail d'éducation et de sensibilisation. Ce changement signifiait que lorsque nous sommes passé.e.s à la fermeture des infrastructures essentielles, il nous a suffi d'élargir le noyau que nous avions formé et d'encourager d'autres bandes à s'organiser de la même manière, en coordonnant les différents rôles par le biais d'une réunion de représentants de chaque groupe cautionné.

(Ce modèle d'organisation, comme tous les autres modèles, vient évidemment avec ses forces et ses faiblesses. Mon intention dans ce texte n'est pas de faire l'apologie d'une manière de s'organiser en particulier, bien que j'aie plus d'expérience avec certaines qu'avec d'autres.)

Avant d'approfondir des idées et des pratiques spécifiques, je veux parler d'une objection courante que les gens ont à l'égard des discussions sur la culture de sécurité dans leur organisation : « Je ne fais rien

fait des recherches sur ces plateformes, ils n'ont rien trouvé. Ces pratiques de sécurité informatique fonctionnent lorsqu'elles sont utilisées correctement et de façon constante. Il y a une vraie différence dans le résultat lorsque nous les utilisons et lorsque nous ne le faisons pas. Ces méthodes nous mettent en confiance lorsque nous nous connectons avec les autres et contribuent à construire la confiance.

Merci d'avoir lu ce texte! Ce texte est plus long que prévu, mais j'espère qu'il a été utile. J'ai écrit cela, car il n'y a pas une tonne de bonnes ressources à propos de la culture de sécurité. Je souhaite que les gens soient inspirés de discuter de quels types de pratiques est approprié pour elleux, animés par un esprit d'assurance, de courage, de connexion et de confiance. Gardons le cap sur le monde que nous tentons de créer par nos actes plutôt que de craindre le mouvement de nos ennemies. Bonne chance!

d'illégal donc je n'ai pas besoin de penser à la sécurité ». Cela pourrait se présenter d'une manière plus spécifique, comme : « je ne parle de rien d'incriminant, inutile de m'inquiéter de la surveillance », ou « En général, je ne me fais pas arrêter à la frontière, donc je n'ai pas à me soucier des piles de journaux anarchistes dans ma voiture », mais l'objection sous-jacente est la même.

C'est l'État et nul autre qui décide de réprimer ou de perturber les gens qui s'organisent – cela n'a pas nécessairement beaucoup à voir avec des actions considérées comme criminelles. Personnellement, j'ai eu un certain nombre de condamnations criminelles : j'ai passé environ un an en prison, deux ans en détention à domicile, et à peu près cinq ans avec diverses conditions de liberté. Toutes ces condamnations étaient pour des tâches d'organisation de routine que l'État a choisi de cibler par la répression pour ses propres raisons. J'ai été condamnée à huit mois de prison pour avoir facilité des réunions et pour avoir écrit et distribué un appel à une manifestation dans le contexte d'un grand sommet ; quelques années plus tard, j'ai été condamnée à un an pour avoir distribué un tract annonçant une manifestation et y avoir ensuite participé. Dans ces deux cas, il y a eu des destructions de biens lors des manifestations, mais je n'en ai jamais été accusée. L'État a plutôt choisi d'utiliser des accusations de complot pour cibler des gens s'organisant de manière visible et routinière comme je l'ai fait à maintes reprises. Une dynamique similaire s'est manifestée dans d'autres affaires de conspiration aux États-Unis et au Canada. Mon expérience n'a rien d'exceptionnel.

Je ne raconte pas ça pour me positionner comme victime – je veux m'organiser pour menacer le pouvoir, donc il me semble logique d'être ciblée pour ça. L'important, c'est que l'État choisisse de criminaliser la distribution de tracts et la facilitation de réunions afin d'intimider ou de faire des exemples. Même si ce genre de répression ne se produisait que dans 1% des cas (même si ça semble arriver souvent), on doit faire attention et s'organiser en conséquence avec des pratiques sécuritaires adaptées. Sinon nous n'aurons plus qu'à restreindre nos propres activités de manière préventive, intérioriser cette répression et intégrer la crainte

et la faiblesse à nos pratiques.

Cependant, la culture de sécurité ne consiste pas seulement à se protéger des accusations criminelles. Il s'agit d'empêcher que nos activités soient perturbées. La criminalisation est une menace particulière, mais c'est loin d'être la seule.

Pendant le grand sommet où j'ai été accusée de complot, seulement deux des 16 agent.e.s d'infiltration du JIG étaient impliqué.e.s dans l'affaire. Les autres avaient changé des mots de passe de sites Web et d'adresses électroniques, dirigé des autobus vers les mauvais endroits, volé des fournitures médicales, répandu des rumeurs nuisibles pour aggraver le conflit social, et même tenté de piéger des jeunes dans un étrange complot à la bombe. Toutes ces actions policières ont eu un effet extrêmement perturbateur, sans jamais avoir besoin de recourir au pouvoir des tribunaux, et nous n'aurons probablement jamais une idée complète de leur impact.

Nous avons déjà vu que le maintien de l'élément de surprise est souvent une considération importante en matière de sécurité. Un exemple dans notre région est l'organisation de manifs de bruit en soutien aux personnes incarcérées : en les organisant discrètement, nous pouvons avoir une liberté de mouvement et d'action pendant un certain temps avant que la police ne soit en mesure de monter une intervention. Ou imaginons qu'une section de l'IWW tente de faire une campagne Réclame ta paye contre un patron – ielles devront prendre des mesures pour se protéger contre les poursuites civiles ou le risque d'être ciblé.e.s par une compagnie de sécurité privée. Ou voyons encore le travail que font les antifascistes pour identifier l'extrême droite – ielles doivent se prémunir contre la divulgation de leurs propres informations personnelles et contre les violences dont ils pourraient faire l'objet dans la rue. Enfin, de plus en plus de compagnies engagent des firmes de sécurité privées pour défendre leurs intérêts d'une manière que la police ne peut pas ou ne va pas faire, ce qui est arrivé à plusieurs reprises ces dernières années dans les luttes de défense de la terre menées par les autochtones.

Les préoccupations en matière de sécurité sont déjà en grande

iPhone sont chiffrés par défaut). Pour les données enregistrées sur les ordinateurs, les disques durs externes, les clés USB ou en ligne, je recommande VeraCrypt. Ça vous permet de faire des « boîtes » chiffrées où vous mettez vos fichiers. Par contre, cela ne vous aidera pas si votre chiffrement est déchiffré au moment ou votre ordinateur est capturé. Si vous croyez que vous pourriez être arrêtés, ne circulez pas entre différents endroits avec votre téléphone (chiffré) allumé. Considérez de dénicher un vieux réveille-matin. Ainsi, vous pouvez éteindre vos téléphones et vos ordinateurs durant la nuit (ce qui remet le chiffrement, typiquement désactivé au démarrage, en fonction), spécialement si vous êtes à risque d'une fouille de votre maison. Faites des sauvegardes de vos données et gardez-les dans un autre lieu.

Trois : Cachez votre identité en ligne lorsque c'est possible. Votre adresse IP est visible pour tous les sites web ou les services que vous utilisez et lie vos activités ensemble devant les yeux de votre fournisseur d'internet et de l'État, même si vous faites des efforts pour protéger votre vie privée en utilisant la navigation privée. Je recommande l'utilisation de TOR pour toute navigation ou recherche. Les médias sociaux corporatifs bloquent généralement TOR (Reddit est une exception et Twitter vous laissera utiliser TOR si vous le leur demandez), donc si vous essayez d'avoir un compte anonyme, une option est d'utiliser un VPN – il y en a un gratuit et disponible sur riseup.net pour l'usage des anarchistes et des activistes.

Beaucoup plus de choses peuvent être faites pour la sécurité informatique, mais ces trois étapes feront déjà une grosse partie de la tâche. Il y a quelques années, la police a fait une décente chez nous. Ils ont capturé une quinzaine d'ordinateurs portables et de téléphones ainsi que plusieurs clés USB et disques durs. Parmi cela, un seul ordinateur portable n'était pas chiffré puisqu'il était resté allumé. Mais du reste, aucune information n'a pu être récupérée. Les historiques de messages textes et d'appels qui ont pu être accédés par nos compagnies de téléphone n'ont rien révélé puisque nous utilisons le chiffrement de bout en bout avec un service qui protège les métadonnées. Nous n'utilisons pas les médias sociaux ou Google pour communiquer. Lorsqu'ils ont

des pages que nous administrons et nous les déplaçons vers une autre plateforme dès que nous les recevons. Nous utilisons des comptes partagés quand cela est possible et nous réduisons la causalité qu'un compte soit relié à des informations personnelles. Peut-être que vous ne voulez pas aller aussi loin, peut-être que vous voulez aller plus loin, mais cela est une façon d'utiliser la puissance des médias sociaux tout en évitant les désavantages massifs.

Une transition de nos usages des médias sociaux peut advenir graduellement, percevoir nos usages de ceux-ci de façon critique et déplacer ces usages surtout vers des rencontres en personne et ensuite vers d'autres plateformes, pièce par pièce. Ça a pris beaucoup de temps pour tant de nos vies pour être capturées par ces entreprises dégueulasses. Ça nous en prendra peut-être beaucoup pour développer de nouvelles habitudes d'organisation et une culture qui leur résiste.

Finalement, parlons un peu de technologies de sécurité. Le sujet est complexe et c'est facile de s'embourber. Néanmoins, il y a quelques étapes simples que l'on peu prendre pour améliorer notre sécurité informatique. Voici trois points.

Un : Utilisez le chiffrement de bout en bout à moins que vous ayez une raison de ne pas le faire. Cette technologie peut être compliquée, mais maintenant, plusieurs applications existent qui rendent leur utilisation aussi facile que la messagerie conventionnelle. Je recommande Signal, de Open Wisper System, même si WhatsApp utilise le même type de protocole de chiffrement, mais sans protection des métadonnées. L'inconvénient est que ce ne sont pas des logiciels multiplateformes, alors qu'avec PGP, puisque c'est possible de copier-coller des blocs de textes, on peut l'utiliser avec tout – les différents clients de messagerie, Facebook, Twitter et même les messages textes. Mais c'est plus difficile de commencer et l'expérience a démontré que les gens ne sont pas prêts à mettre beaucoup d'efforts dans leur sécurité informatique.

Deux : Chiffrez les données où elles sont enregistrées. À moins d'avoir une raison de ne pas le faire, vous devez immédiatement chiffrer vos téléphones cellulaires (Android a une option pour cela, plusieurs

partie intégrées dans nos modes d'organisation. Pour bâtir une culture de sécurité, il faut évaluer les risques de manière explicite au-delà de quelques actions spécifiques, et adopter des pratiques claires conçues pour nous garder en liberté et assurer l'efficacité de nos actions, quelles que soient les formes que prennent nos activités. Pour ce faire, il faut mettre l'accent sur la mise en place de liens solides, tout en créant un climat de confiance où il est possible d'agir avec assurance.

Voici selon moi quelques principes de base de culture de sécurité :

Les deux jamais. Même s'ils sont relativement bien connus, ces deux points sont aussi quelque peu inadéquats. Dans leurs formes les plus simples, ils seraient : « Ne jamais parler de sa propre implication dans une activité illégale. Ne jamais parler de l'implication de quelqu'un d'autre dans une activité illégale. »

Mais cela dissone, car la majorité de ce que l'on fait n'est pas illégale. On pourrait donc reformuler les deux jamais comme : « Ne jamais parler de l'implication d'une personne dans une activité qui risque d'être criminalisée. Ne jamais parler de l'intérêt d'une personne pour une activité criminalisée. »

Toutefois, cette reformulation est encore inadéquate, parce qu'on n'est pas seulement concernés par les accusations criminelles. Bien entendu, avoir des balises claires sur lesquelles tout le monde s'accorde de ne pas raconter de rumeurs et de potins à propos d'actes illégaux est une excellente idée, peu importe dans quel milieu on se trouve. Ceci inclut ce qu'on croit parfois être des blagues – des paroles en l'air qui parlent de combattre les flics ou d'attaquer la propriété privée semblent moins légères lorsqu'elles sont notées dans le cahier d'un infiltré.

L'une des raisons les plus communes qui font qu'on commence à douter de quelqu'un est quand cette personne tente de nous parler individuellement de tactiques illégales. Plutôt que de dire : « Cette personne est une police qui tente de me poser un piège », on peut reformuler nos propos et dire : « J'ai besoin de clarifier ma compréhension de la culture de sécurité avec cette personne si nous continuons à travailler ensemble ». Ainsi, la reformulation des deux jamais peut être une façon simple de faire passer le message. Cela nous aide aussi

à nous souvenir de ne pas spéculer sur les potentiels auteurs ayant pu réussir de telles actions anonymes qui apparaissent autour de nous. Ça, c'est le rôle de la police. Si autour de nous, les gens se demandent qui sont derrière des actions illégales anonymes, on peut leur rappeler simplement que ces actions sont anonyme. Ce n'est pas important de savoir qui les a faits et l'action parle pour elle même.

(Une chose que l'on parle moins est comment les reproches autour de la culture de sécurité peuvent renforcer des dynamiques de pouvoir négatives. Nous devons absolument parler entre-nous des interactions qui nous posent problème du point de vue sécuritaire, mais cela devrait toujours être mutuel et fait en privé si possible – décris ce que tu as entendu, présente ton idée de culture de sécurité , demande si l'autre pense que c'est une limite raisonnable, sois prêt.e à entendre son désaccord. L'objectif est de construire une compréhension partagée pour élargir les formes d'organisations dans lesquelles nous pouvons nous engager ensemble, sans faire sentir les personnes honteuses (ou sans nous faire sentir nous-mêmes plus hardcore). L'une des formes encore plus extrêmes de cela est de faire courir des ragots comme quoi quelqu'un.e serait un.e informateur.trice sans preuve à l'appui, ce qui peut avoir de grandes conséquences sur la vie des gens et qui a fait partie des causes de l'éclatement des mouvements révolutionnaires des années 1970. Un moindre exemple peut être qu'une personne plus « expérimentée » en rabaisse d'autres devant un groupe pour avoir parlé d'actions qu'ielles ont trouvé inspirantes ou parce qu'ielles parlent à certaines personnes.)

Un autre point est de privilégier les rencontres en face à face. Peu importe la plateforme ou à quel point elle est sécuritaire ou pas, nous construisons une meilleure confiance, des relations plus solides et nous prenons de meilleures décisions quand nous prenons le temps de nous rencontrer en personne. Quand les moyens de communication électroniques remplacent le face-à-face, nos conversations sont plus faciles à surveiller, il y a plus de malentendus et elles peuvent être perturbées par des décisions ou des problèmes liés à des compagnies loin de nous. Chaque fois que tu utilises les communications électroniques

notre travail peut être facilement perturbé par la mauvaise presse.

Le contrôle des plateformes par les corporations en est un autre facteur. Facebook est une corporation énorme et riche dont les intérêts sont opposés aux nôtres – ce qui est bon pour nous est mauvais pour eux. Si nous dépendons de leurs infrastructures, ils ont la discrétion de nous mettre à terre à n'importe quel moment pour n'importe quelle raison. De telles entreprises sont très sensibles à la pression du public. On n'a pas besoin de penser pour trouver des exemples de projets qui sont devenus impopulaires et qui ont perdu leurs pages et ainsi, leur capacité à rejoindre leur base. Si nous sommes trop dépendants de ces corporations, ça peut être un désastre. Demandez-vous ce que vous feriez si tout si toutes vos pages et vos comptes disparaissaient ce soir – comment vous organiserez-vous demain?

Il y a aussi le problème de la surveillance, qui ne devrait pas être une controverse. Tout ce qui est écrit sur Facebook est sauvegardé pour toujours dans une base de données à laquelle la police peut avoir accès en tout temps. Le logiciel Facebook (tout comme Google et d'autres) vous traque et vous espionne sur votre appareil. Ces informations sont aussi accessible aux agences renseignement et de sécurité. Cela n'est pas une théorie. Ça a été prouvé à maintes reprises. Les accusations contre ces activistes qui comptent sur ces moyens de partager l'information sont devenues de plus en plus courantes à travers l'Europe et l'Amérique du Nord ces dernières années.

Ma proposition pour les médias sociaux est la suivante. Privilégier les rencontres en personne et les avoir souvent si c'est possible, ainsi, le prochain rendez-vous est déjà prévu dans le cas ou la communication en ligne est perturbée. Quand on utilise les médias sociaux, demandons-nous si c'est vraiment nécessaire si c'était possible d'utiliser une autre plateforme pour cette conversation. Je vous encourage à penser qu'un média social est comme un mégaphone, une façon d'amplifier votre voix. Ce n'est pas comme dans un salon où on discute et on apprend à connaître les gens. Utilisez-le pour promouvoir, pour annoncer, pour disséminer, mais faites bouger les conversations ailleurs. Dans ma propre façon de m'organiser, j'efface presque tous les commentaires

pratiques de sécurité est une étape importante, tout en étant ouvert aux initiatives individuelles par des membres qui s'associent sur des bases affinitaires. C'est-à-dire que la structure d'organisation doit être assez flexible pour accommoder différentes formes d'organisations pour différents types d'activité.

Par contre, en pratique, de telles objections à la culture de la sécurité adviennent maintenant lorsqu'il s'agit de l'usage des médias sociaux desquels Facebook est encore le plus populaire. J'aimerais offrir quelques critiques de l'organisation par Facebook et offrir une proposition de comment les grosses organisations qui en dépendent pourraient faire autrement.

Le point crucial est que les médias sociaux corporatifs réduisent les champs de possibilités pour s'organiser. Puisque c'est à peu près aussi privé que de s'organiser dans la salle d'attente d'un poste de police, aujourd'hui tout le monde le sait, il y a des limites strictes de ce qui peut y être discuté. Ce qui veut dire que si nous sommes dépendants de Facebook parce que c'est notre principal moyen d'organisation, les limites de ce qui peut être pensé et planifié deviennent nos propres limites. Ce genre de désarmement préventif est une position de faiblesse réelle.

De telles plateformes sont aussi vulnérables d'être submergées de réactions hostiles. Nous ne pouvons pas contrôler comment nos actions seront reçues. Parfois, ce que nous faisons n'est pas très populaire – après tout, nous voulons un monde sans capitalisme organisé selon des bases radicalement différentes. Le choc des réactions sur internet après une action impopulaire peut être déstabilisant. Lors d'une récente mobilisation antifasciste dans ma ville, l'extrême droite et les médias de masse ont réussi à provoquer un contrecoup contre les antifascistes qui a inondé les médias sociaux de menaces et de rage. Les antifascistes dépendaient fortement de Facebook pour s'organiser et ielles ont dû faire face à un choix : rester hors ligne et éviter le contrecoup, mais être isolé de leurs camarades ou aller en ligne et discuter avec les gens, mais en ayant des conversations dominées par le stress et l'hostilité. Cette dynamique rend l'organisation beaucoup moins résiliente signifie que

pour t'organiser, demande-toi si cela remplace les rencontres face à face. Si c'est le cas, demande-toi si c'est vraiment nécessaire. Considère de réduire ta dépendance à ces outils et retourne le plus possible vers les conversations en personne. (On reviendra sur la technologie un peu plus loin…)

Une des objections à cela est que beaucoup de gens vivent de l'anxiété sociale et préfèrent communiquer avec leurs appareils; une autre c'est que de se déplacer physiquement est impossible pour certaines personnes. Comme pour d'autres sujets difficiles qui émergent quand on parle de culture de sécurité, je vous encourage à faire face à cette difficulté et à chercher d'autres moyens d'accommoder ces besoins en essayant tout de même de prioriser les rencontres en personne. Après tout, ces technologies sont très récentes et les gens ayant des handicaps de toutes sortes ont développé des moyens depuis longtemps pour se retrouver et s'organiser à propos de sujets qui les affectent.

La répression est inévitable, ou essayer de l'éviter à tout prix ne vaut pas la peine. Peu importe la lutte, si elle est menée au-delà des limites de la légalité, elle deviendra une lutte contre la police. C'est elle qui défend ce monde tel qu'il est. Si nous partons avec l'idée que nous éviterons la répression à tout prix, nous n'utiliserons que des formes de luttes approuvées par la police, ce qui rend quasi impossible la construction d'un pouvoir collectif capable d'un changement transformateur. Si nous n'acceptons pas ces limites, nous devons être prêt.e.s à faire face à la répression.

Une façon de s'y préparer est de mettre la police et les prisons au centre de nos luttes dès le départ. À ce sujet, nous pouvons apprendre des mouvements antiracistes qui gardent toujours en tête la violence raciste et physique de ces institutions et cela même lorsqu'ils choisissent de s'engager dans des thèmes variés . L'avantage est que nous avons déjà élaboré une culture de lutte qui n'est pas choquée par la violence policière et qui est réaliste quant à la prison. Nous pouvons aller un peu plus loin et incorporer des pratiques de solidarités dans nos luttes . Nous nous organisons peut-être dans un lieu de travail; si c'est le cas, intéressons-nous aux luttes de travailleur.euse.s ailleurs et réfléchissons

à des actes de solidarité à mettre en pratique avec celleux qui font face à la répression. Nous nous organisons peut être dans les milieux queers; trouvons et soutenons des prisonniers queers, ainsi nous connaîtrons un peu mieux les prisons dans notre région au moment venu ou nous aurons besoin de ces connaissances. Si nous nous intéressons aux luttes environnementales et de défense de terre, il y a des défenseur.e.s de la terre en prison qui font face à des accusations et à la violence physique de l'État à travers tout le continent ; incorporer des pratiques de solidarité avec elleux dans nos projets peut donner une puissante inspiration à de la résistance forte et courageuse.

Un autre des points positifs est que nous recevrons probablement plus de solidarité en retour puisque la prison est une grande force unificatrice qui lie toutes les formes de luttes contre la domination et l'oppression. Prendre part à une culture de la résistance qui démontre de la solidarité active face à la répression peut jouer gros dans le fait de nous garder en sécurité. De plus, c'est en ayant de l'information véridique que nous combattons la peur . Plus nous en savons à propos du fonctionnement de la police et des prisons, plus nous pouvons transformer notre peur en préparation et en confiance en nous-même.

Avec cela en tête, observons plus en détail ce que signifie d'évaluer le risque. Ce qui importe ici est de le faire ouvertement et avec de la continuité puis de focaliser sur comment rendre possible les actions que vous pensez efficaces et appropriées. Ça peut être facile d'être dans un état d'esprit réticent au risque et de s'autopolicer encore plus de ce qu'a l'État comme capacité de nous contrôler. Être explicites quant au risque peut faire en sorte que ce soit plus facile de mettre l'accent sur le courage et les possibilités.

Si vous vous assoyez pour planifier une manifestation, pensez au ton qu'elle prendra. Anticipez-vous qu'elle sera calme et ordonnée? Ou combative et incontrôlable? Si la police tente de vous bloquer, resterez-vous passifs où essaierez-vous de défoncer leur ligne? Y a-t-il des actions que vous seriez excités de voir advenir durant la manifestation, mais qui risquent d'être criminalisées plus que l'acte de prendre la rue? Cela peut être aussi simple que de poser des autocollants ou bien ça

mais il advient très souvent dans notre milieu que des gens se sentent inconfortables à cause du comportement patriarcal des hommes. Parfois, les gens vont développer des soupçons envers ceux qui les rendent inconfortables de cette façon. Cela est compréhensible, mais c'est une erreur de chercher des infiltrés lorsqu'il y a du sexisme juste devant nos yeux. C'est mieux de confronter les comportements destructeurs en eux-mêmes et si cela nous aide à éviter des informateurs comme Darby, c'est encore mieux.

Un mot sur les organisations de masse formelles. Ces types d'organisations sont souvent très résistantes aux conversations sur la culture de sécurité, car ces discours sont plus communs dans des formes d'organisation qui diffèrent de ce à quoi ils aspirent. La culture de sécurité peut avoir davantage l'air d'une critique générale de leur organisation qu'une proposition de comment la rendre plus solide. Certaines des pratiques ci-haut ne s'appliquent peut-être pas aux organisations de masse formelles, mais j'argumenterais que tous les principes généraux s'appliquent. En fait, je crois que si de telles organisations observent comment elles opèrent, elles verront que des pratiques de sécurité y existent déjà.

Par exemple, dans des chapitres du IWW, il est fréquent de s'organiser discrètement en milieux de travail. Les gens impliqués dans le soutien des organisateur.trice.s qui travaillent sur les lieux utiliseront peut-être des noms codés avec celleux qui ne sont pas directement impliqués ou ne rendront publiques que les informations générales. C'est aussi commun pour certaines organisations de créer des comités plus petits pour prendre en charge des taches plus spécifiques comme d'organiser une manifestation. Leurs discussions ne seront peut-être pas ouvertes à celleux qui ne sont pas impliqué.e.s ou ils utiliseront peut-être d'autres canaux de discutions. Par exemple, ils peuvent éviter les listes de courriels ou les médias sociaux.

Ce que je suggère, c'est que des conversations explicites à propos du risque et de la sécurité soient incorporées dans les différents types de projets menés par ces organisations puisqu'elles ont différents besoins. La formation de comités autonomes qui décident de leurs propres

jamais en posant des questions à propos des activités criminelles de d'autres. Quiconque ayant été impliqué dans la sous-culture activiste peut facilement lister les mauvaises dynamiques qui s'y trouvent.

Comme j'ai dit plus haut en parlant des situations sensibles et complexes liées à la vérification d'identité, nos difficultés liées aux mauvaises dynamiques et à l'oppression dans nos milieux sont des points faibles que la police et le renseignement connaissent de plus en plus. J'ai mentionné la flic qui prétendait être une survivante de violence conjugale pour s'ouvrir un chemin dans la vie des gens (elle était même devenue colocataire chez des copains). Une autre expérience d'infiltration impliquait un flic dans la quarantaine à la peau foncée. Lorsque les gens parlaient de comment celui-ci les rendait inconfortable (entre autres pour avoir brisé les deux jamais), il arrivait à détourner ces préoccupations en répondant qu'ils étaient racistes envers lui. Il a trouvé un groupe d'activistes antiracistes dans une autre communauté que celle qu'il ciblait le plus pour le soutenir et il a réussi à résister à plusieurs efforts pour l'expulser des espaces d'organisation. Il a fini par témoigner dans un dossier qui a envoyé six personnes en prison. Il a sans doute vécu du racisme dans notre milieu, mais cela, avec sa manipulation cynique de l'antiracisme, devrait nous pousser à examiner les faiblesses de nos politiques antiracistes. Avoir des politiques claires à propos de la race, du genre et d'autres oppressions (cela signifie d'être à l'aise de parler en détail de votre analyse devant elleux et pourquoi) ainsi que des pratiques pour adresser ces problématiques de front quand elles adviennent peut diminuer les chances que ce genre de petits jeux fonctionnent.

Plusieurs raisons peuvent faire en sorte que quelqu'un ne soit pas de confiance et multiples de ces comportements prédateurs ne signifie pas qu'une personne soit un agent secret. Un exemple est le cas de Brandon Darby. Dans le texte « Pourquoi les misogynes font de bons informateurs », les auteurs affirment que les gens auraient dû faire plus d'efforts pour confronter les comportements sexistes terribles de Darby avant même qu'il commence à coopérer avec le FBI, alors que plusieurs personnes se sont fait arrêter. Darby est un exemple extrême,

peut être de faire des graffitis ou de briser des fenêtres. Votre plan sera-t-il menacé si vous perdez l'élément de surprise? Qui serait mieux de ne pas être au courant de ce plan? Comment allez-vous joindre les personnes que vous devez contacter sans risquer que les mauvaises personnes aient vent de l'initiative? Communiquer clairement à propos du ton que prendra une action peut aider les autres à élaborer des plans autonomes appropriés.

C'est important d'évider le laisser-aller ou de prendre les choses pour acquis. Voici un exemple de 2018 :

Les organisateur.trice.s d'une foire du livre ont décidé de lancer un appel à une manifestation de soir après l'événement. Ielles ont mis beaucoup d'énergie dans les autres aspects de la journée et étaient complaisant.e.s quant au risque que comportait la manif, parce qu'ielles avaient organisé une centaine de manifs auparavant. Néanmoins, la manif a été beaucoup plus combative que toutes les autres et il y a eu beaucoup de destruction de propriété – ielles n'avaient pas évalué le risque explicitement et n'avaient pas pris le temps de le considérer alors que l'heure du rendez-vous approchait. Ielles n'avaient pas non plus pris pour compte que le JIG focalisait sur un sommet du G7 qui allait avoir lieu dans une autre province cet été-là et que ça pouvait faire en sorte que des ressources policières additionnelles les ciblaient durant cette période. Ceci dit, leurs pratiques de la sécurité dans l'organisation de cette manif n'étaient pas adaptées au niveau de risque que l'action a fini par comporter et tous les organisateurs de la foire du livre ont été accusé.e.s de conspiration.

Cela est un exemple extrême, mais des imprévus vont toujours advenir et cela est généralement une bonne chose, vu que nous ne pouvons pas totalement prévoir notre chemin vers les situations insurrectionnelles. Rester actif.ve dans notre évaluation du risque peut signifier que nous avons moins de chances d'être pris par surprise. Mettre régulièrement en pratique une culture de la sécurité rigoureuse peut réduire les dommages lorsqu'une situation similaire advient. Dans ce cas, une bonne pratique de sécurité informatique, une culture de la non-coopération avec la police, une solidarité persistante et active,

se masquer efficacement et refuser de lâcher ou de se soumettre ont fait en sorte que cette situation inattendue s'est avéré beaucoup moins dommageable qu'elle aurait pu l'être et les personnes ont surmonté la situation avec la tête haute.

Un autre exemple peut être de développer une organisation de masse, par exemple, une organisation antifasciste. Quels genres de questions devons-nous nous poser quant aux risques même en l'absence de planification d'une quelconque mobilisation? Quel niveau de confiance avons-nous besoin entre nous par rapport aux genres de choses que nous voulons faire? Nous risquons peut-être d'être infiltrés par la police donc savoir que nous sommes tous les personnes que nous prétendons être peut être important. Nous pouvons aussi être concernés par l'infiltration de l'extrême droite. Dans ce cas, comprendre nos idées entre compagnons et construire graduellement de la confiance en escaladant tranquillement les niveaux d'actions peut être une solution. Notre principe favorisant l'organisation en personne plutôt que l'activité en ligne rendra probablement plus facile d'achever ces deux objectifs.

Si l'intention est de construire les capacités pour des actions dans les manifs, une partie des conversations sur la sécurité peut être sur la discipline et comment faire des plans. Quelles sont les attentes des un.e.s envers les autres dans des situations tendues? Il est difficile d'honorer les attentes lorsque celles-ci sont vagues. C'est aussi plus facile d'être intelligents quand on a un plan clair pour ce qu'il y a a faire et que nous pouvons juger de si ce plan fonctionne ou pas. Développer de bonnes habitudes d'organisation pour savoir quoi considérer en groupe a d'énormes conséquences pour la sécurité dans la rue – ce n'est pas la culture de sécurité, mais ces discussions sont liées de prêt. Par exemple, les risques de l'organisation antifascistes peuvent inclurent d'être trop peu nombreux.ses, être encerclé.e.s ou séparé.e.s, être suivi.e.s ou identifié.e.s par l'extrême droite ou par la police, subir des blessures inutiles ou se faire arrêter.

Des pratiques d'organisation pour la mobilisation qui tiennent compte du risque incluent un nombre minimum de participants (l'ac-

pratiques peuvent s'adapter aux besoins de divers types d'activité. L'organisation informelle sur des bases affinitaires est un modèle développé pour répondre à ce besoin. Dans un réseau informel (ce qui veut dire sans forme fixe), les individus communiquent leurs idées et leurs intentions puis des groupes affinitaires se forment autour d'un projet quelconque ou d'un désir partagé d'intervenir sur des bases communes. La force de ce modèle est qu'il est très facile d'initier des projets avec des niveaux de risques variés, chacun avec sa culture de sécurité adaptée. Cela implique aussi qu'il n'y ait que les gens concernés qui connaissent les détails ou qui sera impliqué, à moins qu'il en soit décidé autrement.

Une flexibilité semblable peut être incorporée dans d'autres modèles d'organisation. La clé est de respecter et de légitimer les initiatives individuelles, en n'exigeant pas que chaque activité soit approuvée par une entité centralisée (cela peut aussi se faire dans des groupes activistes peu structurés, ce n'est pas une règle réservée aux groupes ayant des processus décisionnels fixes). Il y a aussi le respect pour l'association volontaire. C'est-à-dire de percevoir comme normal le fait de travailler ensemble en petits groupes choisis aux côtés de groupes plus larges ayant des structures plus ouvertes. En terme formel, cela peut ressembler à des comités ou à des groupes de travail ayant l'habileté de définir leurs propres standards de participation. Ça peut aussi être d'avoir une ouverture à certains éléments de l'organisation affinitaire décrite plus haut ou d'être explicite quant à quelles informations doivent être partagées.

Finalement, adresser les mauvaises dynamiques de façon proactive est généralement une bonne habitude à avoir, mais comme c'est tellement important pour la sécurité, l'emphase devrait y être mise dans chaque conversation sur la culture de la sécurité. Plusieurs dynamiques peuvent éroder la confiance et rendre l'organisation plus difficile. Le bullying est un exemple. Les comportements oppressifs enracinés dans le patriarcat ou la suprématie blanche, en est un autre. De centraliser les ressources et les contacts faisant en sorte que les projets ne peuvent qu'être initiés par certaines personnes en est encore un autre. Ça peut aussi être de parler contre les autres, de se vanter, ou de briser les deux

actions clandestines, inviter de nouvelles personnes ou présenter un groupe à un autre est délicat et les considérations sont différentes. Le vouching reste une bonne idée, mais il est important de ne pas mettre quiconque à risque en parlant des actions auxquelles ielles ont participé dans le passé. Puisqu'il est nécessaire d'avoir une forte base de confiance pour faire ce type d'actions, ça peut être possible de faire confiance au jugement de quelqu'un sans avoir de détails d'actions spécifiques.

Les cercles de confiance sont surtout destinés aux réseaux informels et à l'organisation sur des bases affinitaires (ce qui correspond à la plupart de mes expériences d'organisation). Ce modèle consiste à écrire les noms des individus dans votre réseau autour d'un cercle puis à tracer différents types de lignes entre ceux-ci pour symboliser les types de relations qu'ils ont entre eux. Une ligne continue pourrait représenter une relation forte et basée sur la confiance. Une ligne brisée pourrait signifier un certain niveau de confiance et une ligne pointillée, que vous ne vous connaissez pas bien. Ce processus collaboratif peut en dire long sur les dynamiques de groupe et rendre visible où il faudrait s'appliquer pour développer de la confiance.

Cela pourrait révéler qu'une seule personne a des relations fortes avec tout le monde et que les relations des autres sont moins solides. Cela voudrait dire qu'il y a un travail à faire pour équilibrer le réseau, ce qui le rendrait aussi plus résistant (dans le cas où cet individu est arrêté, tombe tout simplement malade ou s'épuise) ainsi que plus égalitaire, car la capacité de lancer des projets est liée au nombre de personnes qui font confiance à la personne qui les lance. Cet exercice pourrait également montrer qu'il y a quelqu'un en qui personne ne fait confiance.

Souvent, un infiltré s'approchera d'abord d'une communauté pour ensuite balancer les noms de ses contacts là-bas auprès d'un autre milieu pour s'approcher d'eux. Les pratiques de vouching et de cercles de confiance peuvent nous protéger de cette menace. Au-delà d'identifier des gens hostiles, les cercles de confiance nous permettent de croître la force de nos réseaux en transformant ces lignes brisées en lignes continues autant que possible.

Avoir des structures organisationnelles flexibles veut dire que nos

tion est annulée ou modifiée par un plan de remplacement de moindre intensité si le nombre de participants minimum nécessaire n'est pas atteint), des stratégies de fuite (à quel moment partir, comment le communiquer aux autres, où se séparer, comment éviter d'être suivis, comment vérifier que chacun.e est rentré à la maison sans problème?), des points de rassemblement (se regrouper avant de se rendre vers le site d'une action), des tactiques de rue appropriées (se positionner en deux lignes avec des rôles complémentaires par exemple), des pratiques de communication claires (comment communiquer dans la rue, amènerez-vous vos téléphones, quels noms utiliser entrevous?) et un moment de vérification prévu (comment vérifier entrevous après avoir quitté pour s'assurer que tous sont en sécurité, se rassembler par la suite pour faire un retour sur l'action ou offrir du support).

Les groupes qui s'organisent ont vécu des expériences de culture de sécurité variées et je ne tenterai point de parler de tout. J'aimerais plutôt en partager quelques-unes dont j'ai fait l'expérience avec les gens qui m'entourent et qui sont réussis. Celles-ci comportent la vérification de pièces d'identité, le vouching, les cercles de confiance, les structures d'organisation flexibles et le fait d'adresser de façon proactive les mauvaises dynamiques.

Les vérifications de pièces d'identité, c'est pour établir qu'une personne est bien qui elle prétend être. Dans la campagne contre l'oléoduc décrite plus haut, au moment où nous avons voulu passer à des actions directes plus intenses, nous avions besoin d'approfondir la confiance entre les personnes avec qui on s'organisait. Parce que nous parlions régulièrement de risque, nous avons compris que les pratiques de sécurité utilisées pour des manifestations, des petites occupations et des événements éducationnels n'étaient pas appropriées pour cela. Puisque nous étions préoccupé.e.s par de potentiels infiltrés, nous avons décidé de vérifier nos identités les uns des autres. Cela pouvait être d'inviter quelqu'un à prendre un café et sans avertir, montrer ma carte d'identité et peut-être une photo de famille ou un album de finissant. Je pouvais dire à cette personne que je voulais qu'ielle puisse avoir confiance que j'étais réellement celle que je prétendais être parce que

je voulais que nous développions la capacité de mener ensemble des actions plus risquées. Nous discutions ensuite de ce que cette personne pourrait me montrer. Parfois, il s'agissait d'un coup de fil au travail ou à un membre de la famille sur un haut-parleur. Je pouvais ainsi entendre la voix de la personne à l'autre bout du fil donner des détails sur la vie ou le travail de la personne. D'autres fois, la pièce d'identité était suffisante. Parfois nous nous sommes accompagnés vers nos appartements. L'idée était d'être aussi mutuel.le.s que possible (ce qui est difficile, car en pratique, il y a toujours une personne qui initie le processus) et de maintenir l'accent sur construire la confiance.

C'est inutile de faire de telles vérifications d'identité pour des personnes en qui on n'a pas confiance ou avec qui on ne se sent pas confortable de faire des actions risquées peu importe comment ielles se nomment. Le but n'est pas de trouver des flics, c'est d'approfondir notre niveau de confiance. Vérifier nos identités de cette façon devrait être un signe de respect. Plusieurs facteurs peuvent faire en sorte que ce processus ne soit pas si évident. Par exemple, les gens qui immigrent au pays n'ont peut-être pas de famille à proximité ou le même type de documents. Souvent, les personnes queers et trans n'utilisent pas les noms inscrits sur leurs documents officiels et ielles ne se sentent peut-être pas confortable de partager leurs noms légaux ou de vielles photos. Néanmoins, ce sont des choses à prendre en considérations et desquelles on doit s'adapter. Ce ne sont pas des raisons pour faire des exceptions. Une flic infiltrée dans ma région prétendait fuir une relation abusive et a utilisé les politiques de solidarité avec les survivant.e.s d'agression pour éviter de parler des détails de son passé. Notre inconfort quant aux sujets plus sensibles et complexes crée des angles morts qui peuvent être utilisés par celleux qui nous veulent du mal – nous devons être braves et trouver les moyens d'adresser cette complexité. Nous ne devons pas l'éviter.

Un.e ami.e qui a eu cette expérience a ajouté qu'il y a peut-être des moments où c'est correct d'être moins mutuel, lorsqu'on ne veut pas donner le contrôle de ce que la preuve aura l'air aux gens. Ielle a aussi mis l'accent sur le fait que cela n'aidera pas nécessairement dans

le cas des balances (en opposition aux infiltrés) qui sont bien celleux qu'ielles prétendent être, mais qui ont de mauvaises intentions. On doit aussi avoir une idée claire à l'avance de quoi faire si quelqu'un ne peut ou ne veux pas, ou si quelque chose fait en sorte qu'on doit revoir la confiance qu'on a envers quelqu'un.

Le vouching est une pratique pour intégrer de nouvelles personnes dans un groupe qui existe déjà ou dans un espace d'organisation. Tout comme nos autres pratiques, c'est mieux lorsque c'est explicite et fait de façon constante. La première étape est d'avoir des bases de confiance claires au sein d'un groupe. Peut-être que votre base, c'est que quelqu'un ait des idées compatibles avec les vôtres et soit fiable. Peut-être que vous devez savoir que les personnes sont bien celles qu'elles prétendent être, qu'elles ne paniquent pas en cas de stress, qu'elles ont certaines expériences d'organisation et qu'elles sont confortables avec certains types d'actions. Peu importe ce que c'est, le vouching se rapporte au fait qu'une ou plusieurs personnes introduisent une nouvelle personne et suggèrent explicitement que celle-ci rencontre les bases de confiances déjà définies. Les autres personnes présentes devraient explicitement accepter ou rejeter ce vouch. Être explicite de cette façon évite certains risques de faire implicitement confiance aux gens pour des raisons superficielles, par exemple pour correspondre à des normes de sous-culture ou pour avoir une certaine identité de genre.

Voici un exemple de vouch : « Je connais cette personne depuis cinq ans, durant ce temps, nous avons travaillé ensemble dans des projets publics et je lui fais confiance pour me soutenir dans des moments difficiles. Je suis allé souper chez son père une fois et je suis allé souvent la chercher au travail. » Voici un autre exemple : « J'ai rencontré cette personne l'an passé dans un événement sur les changements climatiques et on s'est vu plusieurs fois à des événements liés à l'environnement depuis. Nous avons souvent discuté sur différents sujets et je l'aime bien. Je sais qu'elle cherche à prendre de l'expérience dans l'organisation d'actions et je crois que ça pourrait fonctionner avec nous. »

Une exception d'être explicite à savoir si vous faîtes confiance à quelqu'un est de ne pas briser les deux jamais. Si vous organisez des