Comment s’organiser en ligne ? Une brochure pour lutter !

Publié le 30 mars 2020 | Maj le 7 avril

En peu de temps, le virus Covid-19 a complètement changé l’organisation de nos luttes. L’incertitude est grande, personne ne sait ce qui nous attend ensuite. Une chose est sûre, les plus précaires sont toujours plus exploité·es et l’étau sécuritaire se ressert encore plus. Face à cela, s’organiser devient encore plus vital. Même si une partie de l’organisation de l’activisme s’organisait déjà à distance depuis longtemps, les réunions physiques, en petit comité ou en Assemblée Générale restaient pourtant le lieu privilégié des prises de grandes décisions. Face à l’impossibilité de maintenir ces réunions physiques, nous souhaitons transmettre ici notre expérience d’une organisation 100% à distance grâce à des outils libres qui garantissent au mieux possible notre sécurité et celle de nos camarades.

Avertissement : Cet article a été écrit dans l’urgence de la situation. Certaines parties ont été volontairement raccourcies, des explications techniques simplifiées et certains tutoriels d’utilisation de logiciel renvoient vers d’autres sites. Nous pensons néanmoins qu’il est important de publier cet article dès maintenant. Nous essaierons de mettre à jour cet article régulièrement. N’hésitez pas à faire vos retours dans les compléments d’infos.

0. Spoiler :

Si vous n’avez pas le temps de lire ce texte qui problématise l’adaptation des outils d’organisation physique au 100% numérique et cherche une solution adaptée à chaque cas spécifique, mais que vous préférez une solution minute pour savoir comment organiser une réunion plus sécurisée que sur Skype ou Discord, on vous conseille :

- Etherpad + Jitsi pour une réunion jusqu’à 10 grand maximum
- Mattermost + Mumble pour une réunion jusqu’à 250 personnes

Pour un maximum de sécurité, utilisez ces outils en vous connectant à internet avec une adresse mail chez Riseup.net et le VPN de Riseup.net

Si vous avez un peu plus de temps, vous pouvez naviguer rapidement dans la rubrique qui vous intéresse grâce au sommaire ! Mais en vrai on vous recommande de lire l’article en entier !!

Sommaire

1. Se rappeler comment on s’organise quand on se voit en temps "normal" (AG, réunion ...)

"L’outil doit s’adapter à l’utilisateur·trice et non l’inverse" est un des préceptes les plus importants à prendre en compte lorsque l’on cherche des outils pour lutter. Il ne va pas s’agir en période de crise de réinventer tout un fonctionnement organisationnel en fonçant tête baissée vers des nouveautés technologiques.

Il faut cibler ses besoins. Or, nos besoins et nos fonctionnements sont en général déjà bien établis et sont le fruit de nombreuses années de test et de retour critique. De l’association sportive aux coordinations nationales de lutte en passant par les syndicats ou groupes affinitaires, chaque collectif possède un fonctionnement qui lui est propre. Pourtant avec le temps et l’habitude, certains fondements dans le fonctionnement d’un collectif se transforment sans qu’aucune discussion formelle n’ait lieu. Changer d’outils va donc nous obliger à non pas repenser le fonctionnement de notre groupe, mais à mettre à plat son fonctionnement actuel, pour ensuite trouver les bon outils permettant de l’adapter à une organisation sans possibilité de se rencontrer physiquement.

2. Comment lister ses usages

Tout d’abord, il faut s’en convaincre, malgré les effets d’annonce, le logiciel couteau-suisse parfait n’existe pas. Même le géant Facebook a dû racheter WhatsApp et Instagram en plus du site originel pour répondre à des besoins auquel il ne pouvait pas répondre. D’autre part, il n’existe en réalité aucune solution totalement "clé en main" à votre problème, il va donc falloir adapter les différents outils (qu’on vous présente plus bas) à vos usages.

Les outils vont devoir s’adapter au public visé et ne pas être excluants. Ainsi malheureusement, généralement, plus on souhaite un degré de sécurité haut, plus il faudra de maîtrise de l’outil. Le problème est que certaines personnes étaient déjà réfractaires à ces outils avant d’être confiné·es et que former des personnes à un nouvel outil à distance s’avère plus complexe que dans une relation physique.

De même, si l’ordinateur personnel chiffré sous Linux connecté avec un routeur [1] qui nous appartient devrait être la norme, nous savons que ce n’est pas le cas. Bien que les magasins d’informatique restent ouverts (pour ne pas pouvoir refuser de télétravailler au pretexte que son ordinateur est en panne), changer de système d’exploitation de son PC seul·e, en se retrouvant potentiellement ensuite sans moyen de revenir en arrière n’est peut être pas la meilleure des idées ... et bien souvent aujourd’hui certain·es ne possèdent même pas d’ordinateur mais uniquement un smartphone pour se connecter.

Il faut donc qu’entre vous, au sein de votre collectif, vous fassiez un listing du matériel de chaque personne et de son niveau de connaissance en informatique. Bien entendu, quand il s’agit d’un collectif plus grand que 10 personnes, cela n’est pas forcément possible, mais on peut en fonction du public visé affiner au maximum les besoins de chaque membre du collectif avant de décider de quel(s) outil(s) choisir.

Ainsi, pour l’organisation d’une AG interprofessionelle de ville regroupant 200 personnes de tout âge et de toutes professions par exemple, on partira du principe que les gens ont le moyen de se connecter le plus mauvais possible et le plus mauvais niveau possible en informatique. Pour une réunion de hackers activistes de cinquante personnes on partira du principe que toutes et tous possèdent le niveau de sécurité maximum... c’est ensuite à vous de moduler entre ces deux extrêmes.

3. Comment adapter cette organisation au confinement

Maintenant que vous avez mis à plat votre fonctionnement et listé vos usages, nous allons partir de cas types pour proposer des solutions d’adaptation de son organisation afin de vous montrer qu’en fait c’est très simple (on ne parle toujours pas de logiciel, toujours de la théorie, si vous voulez allez plus vite allez lire directement ici

3.1 Un exemple type, organiser une AG

Organiser une AG de lutte avec 50 à 250 personnes (de son entreprise, de son université, de son syndicat, de son organisation politique).

Contrairement à ce que l'on pourrait penser, ce cas typique est en réalité le plus simple à transposer sur internet car il est le plus codifié. À partir de ce modèle type très rigoureux, on pourra ensuite décliner d'autres modèles facilement.

Généralement, lorsqu'on organise une grande AG de lutte et qu'on veut qu'elle se passe bien, on procède ainsi pour la répartition des tâches (c'est un exemple type "idéal")

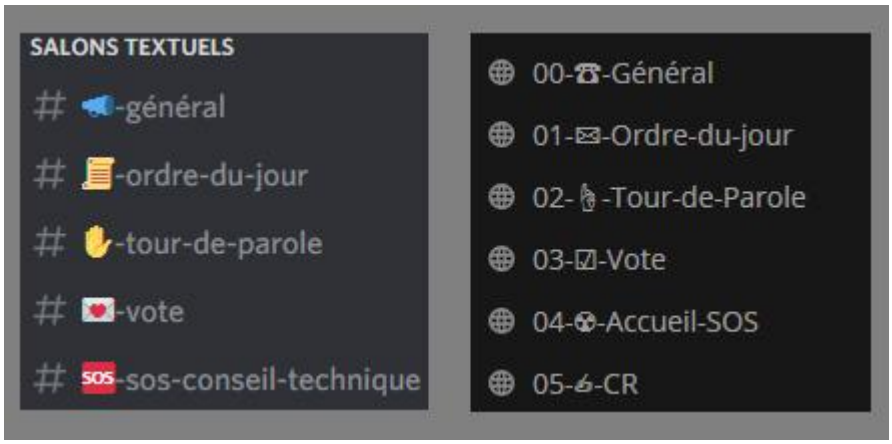
- 2 personnes à la tribune pour animer l'AG
- 2 personnes qui prennent les tours de parole et gèrent le temps de parole
- 2 personnes qui comptent les voix pour les votes
- 2 personnes qui prennent des notes
- 2 personnes qui gèrent les entrées et sorties de l'AG pour à la fois accueillir les personnes qui débarquent et aussi prévenir si un potentiel groupe perturbateur (fachistes, flics) arrive.

En face on a : 200 personnes se sentant plus ou moins légitimes (les mec blanc cis accaparant une bonne partie des interventions), plus ou moins aguerries aux AG, plus ou moins attentives... et des personnes qui vont aller chacune leur tour à la tribune faire leur intervention dans un quasi silence (en dehors de quelques chuchotements)

Au début de l'AG, les postes sont répartis (au vote où à l'auto-designation) et les règles de fonctionnement sont définies (par exemple faut-il une majorité qualifiée ou totale, comment est prise en compte l'abstention, le temps maximum de parole par personne ...)

Un fois passé à l'écrit ce fonctionnement à peu près habituel d'une grosse AG, on voit que c'est finalement très simple à transposer sur internet.
Il suffit en fait de reconstruire la même architecture dans un logiciel de chat (quelqu'il soit).

Concrètement, on crée un canal par rôle et cela donne ça sur mattermost



Ensuite, quel que soit le mode de discussion choisi (texte, voix, vidéo) 1 ou 2 personnes sont désignées pour s’occuper de chaque canal, les règles sont énoncées et normalement ensuite l’AG peut démarrer et roule sans accroc.

3.2 Déclinaison

À partir de ce modèle type on peut décliner aisément des variantes bien plus légères.

Exemple type : organiser une réunion de 5 à 10 activistes qui se connaissent bien pour discuter de comment sauver les licornes du Parc de la Tête d’Or :

On part du fonctionnement de l’AG à 200 et on le transpose à ce petit groupe, ce qui donne :

- 2 personnes à la tribune pour animer l’AG => 1 personne pour animer la réunion
- 2 personnes qui prennent les tours de parole et gèrent le temps de parole => autogestion collective
- 2 personnes qui comptent les voix pour les votes => autogestion collective
- 2 personnes qui prennent des notes => 1 personne qui prend des notes
- 2 personnes qui gèrent les entrées et sorties de l’AG => autogestion collective

Il est très important de noter que certaines tâches ne sont pas simplement supprimées mais sont attribuées à une autogestion collective.
Il faut en effet que le fonctionnement décidé soit clair pour tous le monde au départ de la réunion et qu’il soit clair que la gestion de certaines taches soit collective. Si on se trouve dans un groupe qui se connaît moins bien et a moins de confiance, on peut réassigner des personnes à des tâches comme le tour de parole. On peut ensuite décliner ce modèle de la manière que l’on veut en assignant plus ou moins de personnes aux tâches ou en autogérant collectivement plus ou moins de tâches.

3.3 Adaptation

Il ne s’agit pas par ces modèle type d’imposer quoi que ce soit et de créer un fonctionnement universel. **Il s’agit simplement de partir d’un exemple connu** par le plus grand nombre (pas forcément approuvé, mais connu) et de montrer comment on peut le transposer sur un réseau "virtuel". A partir de là, en fonction de votre organisation habituelle à vous — comme on l’a dit au début de cet article — vous pouvez remettre à plat et par écrit votre fonctionnement et le transposer. L’important étant qu’aucune tâche ne soit oubliée.

En effet, trop souvent l’expérience nous montre que lors d’une réunion à distance, même dans le cadre d’une entreprise brassant des milliers de Brouzouf, les bases du fonctionnement d’une réunion physique sont balayées par "la technologie c’est trop cool" et la réunion virtuelle se termine en cacophonie générale et tout le monde en sort frustré·e.

3.4 Spécificité du virtuel

Il n’y a globalement rien à ajouter de plus au fonctionnement expliqué ci-dessus. Pourtant, nous vous proposons ici quelque Astuces/Tips afin que votre réunion se passe pour le mieux.

Chacun·e doit tester sa configuration avant la réunion ! N’attends pas le dernier moment, la plupart des logiciels sont utilisables même tout·e seul·e simplement pour voir si cela fonctionne

Prévoir un temps au début de la réunion pour que chacun·e soit sûr que sa configuration fonctionne et fasse le cas écheant des tests micro ou caméra (plus le nombre de participant·es est élevé, plus il faut laisser un temps avant durant lequel les personnes qui s’y connaissent le mieux dans le groupe accueillent les participant·es perdu·e·s. Pour 200 personnes, prévoir 1H voire 2H avant, pour 30 personnes 20 à 30mn environ). Dans le cas où le groupe a l’habitude de faire des réunions sur une plateforme, réduisez le temps au minimum (5/10mn), mais ne supprimez pas ce temps, un souci technique inattendu peut survenir !

N’écrivez/parlez/gesticulez pas trop vite. Certaines participant·es de la réunion peuvent avoir une mauvaise connexion à un moment donné (ou pendant toute la réunion), ce qui conduit à de la frustration/énervement quand il manque la moitié des informations. N’hésitez pas à rajouter du temps de parole (30% à la louche) par rapport à une réunion physique pour que les intervenant·es n’aient pas besoin de trop accélérer lors de leurs interventions.

Dites clairement quand vous prennez la parole et la rendez. Même lorsqu’un·e modérateur distribue la parole, il faut le dire, car on ne peut pas hocher la tête ou se lever pour montrer physiquement qu’on a entendu.
Vous pouvez par exemple commencer (à définir entre vous) par : Camille OK - et finir par : Camille Terminé . (Camille étant à remplacer par votre pseudo ou prénom bien entendu, si tout le monde choisit Camille, la réunion risque d’être un peu compliquée en virtuel ;)

En cas de réunion audio, demander à ce que tous les participant·es coupent (mute) leurs micros, et ne l’activent que lorsqu’ils ou elles parlent, cela évitera les bruits parasites.

N’hésitez pas à donnez vos propres Tips dans les compléments d’infos...

4. Quelques informations pour comprendre les outils libres, le chiffrement et les serveurs de confiance.

4.1 Propriétaire VS libre

Avant de rentrer dans le vif du sujet, c’est à dire le choix du/des logiciels de chat. Nous pensons important de faire un point de rappel sur les logiciels libres. Si cela ne vous intéresse pas ou si vous pensez être suffisamment au courant, sautez ce paragraphe.

Skype, Facebook Messenger, Discord, Zoom ou même Snapchat et Instagram sont en soit de très bon logiciel pour chatter.
Plus précisément quand on dit cela, cela signifie qu'ils fonctionnent quasiment sans problème, sur n'importe quelle configuration et que les qualité sonore et vidéo sont très bonnes. Sauf que ce ne sont pas des logiciels recommandables à utiliser, que cela soit dans le cadre personnel, professionel ou activiste, il ne faudrait normalement pas les utiliser (on sait que vous les utilisez et quelleques unes de nous aussi, des fois malheureusement, mais dans l'idéal il faudrait vraiment arrêter !).

Mais pourquoi sont ils.elles si méchant.es avec ces logiciels ces geek activistes alors que ça fonctionne super bien, c'est quoi le souci à la fin ?

Nous ne sommes pas méchant.es. Les méchants, c'est plutôt les GAFAM[Google, Amazon, Facebook, Apple, Microsoft] mais aussi les BATX[Baidu, Alibaba, Tencent, Xiaomi] et bien sûr les Etats et leurs services de renseignement qui veulent mettre leurs nez partout.

Les logiciels présentés ci-dessus sont appelé des "logiciels propriétaires" c'est-à-dire que leurs codes source ne sont pas consultables, vous devez leur faire 100% confiance.

Pour faire simple, c'est un peu la même chose que lorsque vous achetez une bouteille de CocaCola, ou un pot de Nutella : vous ne pouvez pas connaitre la composition exacte de ce que vous allez consommer. On appelle ça "le secret industriel" censé protéger les inventions pour ne pas qu'une entreprise qui aurait dépensé des millions en recherche et développement et en pub se fasse copier (c'est l'histoire qu'on raconte). Sauf que bon, les profits d'une entreprise comme Ferrero (Nutella), ce n'est absolument pas votre problème, par contre votre santé ça l'est. Alors oui (on ne vas pas se mentir) le Coca et le Nutella c'est bon au goût, mais on ne sait pas si c'est bon pour votre corps ni pour la planète (bon en fait on le sait c'est de la merde hein, mais on ne peut pas le prouver à 100% car on a pas la recette).

A l'inverse, quand vous faites une confiture d'abricot avec des fruits d'un arbre que vous avez vous même plantés et dont vous connaissez au départ l'origine de la graine, lorsque vous donnez vos pots de confiture super bon à vos amiès, vous pouvez leur donner la composition exacte en fruits et sucre, vous pouvez leurs garantir l'origine de chaque produit et vous pouvez aussi s'ils ont aimé, leur donner votre recette. Cette recette, ils peuvent l'améliorer, la transformer et la donner à d'autres amiès (ou au monde entier) gratuitement, c'est ce qu'on appelle en informatique, les logiciels libres !

Bon, c'est bien joli ces histoires de nourriture, mais c'est quoi le souci avec la recette secrète des GAFAM ?

Et bien, par exemple on sait que :

- Skype copie toutes les URL que vous partagez pendant une communication et les envoie automatiquement à un serveur pour "faire des statistiques"
- Facebook Messenger a des modérateur·rice-s qui peuvent consulter en direct vos

communicatons et les supprimer
- Discord peut conserver vos données et discussions, les refiler à des tiers si cela lui est demandé et peut fermer un serveur de discussion à tout moment
- Telegram peut fermer un canal public de discussion
- ...

Bref, c’est pour ça qu’on aime bien les logiciels et tous les outils libres, car on veut savoir où sont stockées nos données et ce qu’il en advient et le décider nous même

4.2 Chiffrement et sécurité

Résumer et vulgariser en quelques lignes toute la complexité de la sécurité informatique nous semble bien illusoire. Nous vous proposons ici un très rapide résumé pratique et exemplifié pour permettre au plus grand nombre de se saisir de cette question. Néanmoins, nous ne pouvons que vous conseiller de lire (ou relire) les deux tomes de l’excellent Guide d’autodéfense numérique. Seule une lecture attentive du deuxième Tome de 178 pages vous permettra de comprendre comment garantir votre sécurité numérique dans sa globalité.

4.2.1 Généralité

Généralement, quand on occupe une maison, on ne se contente pas de pousser la porte, on ajoute un cadenas pour se protéger des méchants afin qu’ils évitent de débarquer au milieu de la nuit et on s’assure ensuite de bien refermer quand on sort pour ne pas qu’ils puissent installer des micros dans les murs. Autre exemple, quand on envoie un chèque d’abonnement à un journal par la poste, on le met dans une enveloppe, on ne se contente pas de le scotcher à une carte postale.

Le chiffrement logiciel, c’est un peu la même chose, c’est une couche de protection qui permet aux données d’une communication d’être impossibles à lire ou à écouter si on n’a pas la clé ou le mot de passe pour ouvrir (déchiffrer). Sans cette clé ou ce mot de passe, les informations de cette communication sont des données totalement sans structure, sans aucun sens, incompréhensibles.

Sur l'internet [...] toutes les communication sont susceptibles d'être écoutées.

Sur l’internet, quand on communique (par mail, chat ou appel vocal) en temps normal, c’est un peu la même chose que si on discutait au milieu d’une allée d’un supermarché, toutes les communications sont susceptibles d’être écoutées par celles et ceux qui passent à côté de nous.

L’argument principal de Tonton Danièl·e pour refuser de protéger ses informations est de dire : "de toutes manières je n’ai rien à me reprocher". On a beau lui arguer que ce qui est autorisé aujourd’hui peut être interdit demain et que ses photos avec ses potes en train de picoler pourront se retourner contre lui/elle un de ces jours, rien n’y fait.

Les grosses entreprises du web [...] ont constaté qu'il était bien plus profitable d'utiliser vos

données informatiques que de vous faire payer 5$/mois

Pourtant, il ne s'agit pas de paranoïa, les grosses entreprises du web (les GAFAM et BATX) qui fournissent leurs services sans que vous n'ayez à sortir un centime de votre poche ne sont pas des associations humanitaires. Si elles "offrent" leurs services, c'est qu'elle ont constaté qu'il était bien plus profitable d'utiliser vos donnés informatiques que de vous faire payer 5$/mois. Ainsi, vous leurs offrez gratuitement toutes vos donenées (like, groupes d'amiìes, nombre d'heure d'utilisation, adresse ip, ...) et ces multinationales n'on plus qu'a piocher dedans allégrement pour les revendres aux plus offrants ! Que cela soit à d'autres grosses entreprises pour faire des publicités ciblés ou aux services de renseignements de n'importe quels pays, peu importe tant qu'on peut y mettre le prix ! "Quand c'est gratuit, c'est vous le produit" !

Bref, c'est pour cela que dans la liste des differents outils que l'on vous proposera en dessous, nous vous donnerons prioritairement des logiciel libres n'appartenant pas à ces gros monstres capitalistes et offrant en plus un chiffrement approuvé.

4.2.2 Souriez, vous êtes pisté !

Sur l'Internet, on laisse "des traces" à chaque étape de notre passage. En effet, quand on se connecte à notre Box/Routeur/smartphone, notre fournisseur d'accès (Orange, Free,...) nous attribue une adresse IP. C'est l'équivalent (à peu près) de notre adresse physique, ou notre numéro de téléphone : c'est un identifiant unique. Si certains (rares) fournisseurs attribuent une adresse qui ne change pas (IP fixe), en général ils changent régulièrment notre adresse (IP Dynamique) pour ne pas bloquer des adresses inutilisées pour rien (une adresse IP coute de l'argent à notre fournisseur).

Dans tous les cas, adresse fixe ou dynamique, **votre fournisseur enregistre la correspondance entre votre identité réelle et l'IP attribuée**. Les différentes lois dites de "sécurité et informatique" de l'état Français font qu'actuellement, vos fournisseurs doivent conserver vos différentes IP pendant 2 ans !

D'autre part, comme avec le courrier physique, lorsque l'on envoie un courrier, il transite obligatoirement par La Poste (ou un fournisseur privé). La Poste peut donc théoriquement et même légalement aujourd'hui ouvrir tout votre courrier car de fait, il passe directement par ses services et vous ne pouvez pas y faire grand chose.

Sur Internet, c'est pareil : tous vos échanges sont fait sous forme de "paquets" qui comportent l'adresse de l'expéditeur et celle du destinataire. Ces paquets passent tout d'abord par votre FAI (Fournisseur d'Accès à Internet : Free, Orange, ...) puis divers intermédiaires, avant d'arriver à destination. **Les intermédiaires savent au minimim qui envoie un paquet, à qui, et - s'ils ne sont pas chiffrés - lire leur contenu** et donc vos échanges (lettres d'amour, mots de passe..). Les FAI sont contraints par la loi de stocker pendant 2 ans toutes les adresses des sites internet ou vous vous êtes connecté !

Lorsque l'on consulte un site internet, il est très courant qu'il pose un "cookie" dans

votre navigateur. Ces cookies peuvent ensuite être relus par le site internet la prochaine fois que vous les consultez : quelques semaines plus tard, ou lorsque vous changez de page. Ils aident à vous identifier et savoir par exemple que vous êtes connecté·es à l'espace privé de votre site d'information préféré, connaitre le contenu de votre panier d'achat, mais également à des fins plus malicieuses, qui ne présentent aucun intérêt pour vous.

Il est également possible de vous identifier sans poser de cookie. En effet, votre navigateur envoie une quantité non négligeable d'informations : adresse ip, mais aussi système d'exploitation (Linux, Windows, Mac ...), l'identité de votre navigateur et sa version (Firefox V1312, Chrome V2, ...) ainsi que la taille de votre fenetre de navigateur (800*600, 1280*720 ...), polices de caractère disponibles sur votre système. **Ces informations peuvent être utilisées pour créer une empreinte (fingerprint) unique ou quasi-unique de votre navigateur**, et permettre de vous suivre. Le site "panopticlick" de l'EFF (Electronic Frontier Fundation, des amiìes d'internet) permet de tester l'empreinte d'un navigateurs.

Grace à ces techniques, un site ou service peut vous retrouver et vous proposer par exemple de la publicité ciblée et aggréger des données personnelles sur vous. Et en plus, la loi informatique et sécurité les obligent à conserver ces informations pendant 2 ans.

4.2.2 Le chiffrement, qu'est-ce que c'est concrètement ?

Afin de sécuriser nos échanges, on peut les chiffrer. On utilise pour cela, une (ou plusieurs) clés. L'un des plus vieux codes de chiffrement par clés que vous connaissez peut-être, c'est le « code par décalage », très utilisé par Jules César. Il s'agit simplement de décaler les lettres d'un nombre que l'on a défini avec son correspondant. Par exemple, si on décide que la clé est 3, alors A=D, B=E, W=Z, X=A, etc. Et donc « Bonjour » = « Erqmrxu ». Ce code très ancien est facilement « cassable » car le nombre de combinaisons différentes n'est que de 26. En testant toutes les combinaisons (ce qu'on appelle une « attaque par force brute ») on peut retrouver la clé en peu de temps. (Vous pouvez vous amuser avec ici.)

Aujourd'hui, les clés de chiffrement sont de 128 bits, et il faut théoriquement 2^{128} essais (soit environ 340 milliards de milliards de milliards de milliards) pour pouvoir retrouver la clé par force brute (ce qui techniquement n'est pas possible actuellement).

L'autre contrainte dans ce fonctionnement, c'est que pour que votre destinataire puisse lire votre message chiffré, il doit connaître la clé de chiffrement que vous avez utilisée (dans le cas du code César ci-dessus, la clé à transmettre est donc "3"). C'est ce que l'on appelle la cryptographie symétrique. Bien entendu, donner la clé en même temps que le message chiffré n'aurait aucun sens ; il faut donc la transmettre par un autre canal. César donnait ainsi sa clé à son officier avant sont départ, et une fois sur le champ de bataille, celui-ci reçoit les information codées qu'il peut décoder grâce à la clé qu'il a déjà sur lui. Le problème est que ce sytème n'est pas des plus pratiques.

Un autre système a donc été mis en place, la cryptographie asymétrique, où la clé est divisée en deux parties : l'une, publique, que tout le monde peut connaître, et l'autre, privée, qui n'est connue que du destinataire des messages chiffrés. Dans ce système, n'importe qui qui connaît la clé publique d'une personne peut chiffrer un message pour elle. Mais seule la personne qui connaît la clé privée correspondante est en mesure de le déchiffrer. Du coup, puisque la clé publique seule ne permet pas de déchiffrer les messages, on peut la diffuser en toute sécurité, y compris par des canaux non confidentiels.

4.2.2.1 Utilisation courante : SSL/HTTPS

Si beaucoup pensent encore que le chiffrement, c'est "un truc de geek·ette", en réalité, vous l'utilisez sans même le savoir en ce moment en lisant cet article. En effet, **le "https" au lieu du simple "http" dans la barre de votre navigateur signifie que vous utilisez une connexion chiffrée** (sur les navigateurs sérieux comme Firefox, un cadenas s'affiche même à coté de "https" pour signifier que la connexion est sécurisée).

Concrètement, cela signifie que **grace à ce chiffrement, votre fournisseur d'accès internet (ou votre fournisseur VPN) sait que vous êtes sur une page internet mais ne peut pas savoir ce qu'il s'y passe ni ce que vous y faites**. Ainsi, lorsque vous lisez vos mails en allant sur https://mail.riseup.net, votre fournisseur sait que vous êtes sur ce site mais ne sait pas quel est votre nom d'utilisateur et mot de passe et ne peut pas lire vos mails dans votre dos.

Pour en savoir plus, vous pouvez lire : https://sebsauvage.net/comprendre/ssl/

4.2.2.2 Utilisation plus complexe : PGP/GPG

Si vos mails ne peuvent pas être lus directement par votre fournisseur d'accès internet, ils peuvent néanmoins êtré interceptés par une personne malveillante. On appelle ça une attaque par interception (voir ici)

Le standard OpenPGP est un format de cryptographie qui permet de pallier à cela en chiffrant et de déchiffrer ses emails ou des fichiers par le biais de clés asymétriques. Ca à l'air compliqué dit comme ça, mais en fait il y a des logiciels libres de gestion des mails comme Thunderbird qui sont assez simples d'utilisation et permettent de protéger très efficacement nos communications.

Pour en savoir plus, vous pouvez lire : "Comment chiffrer ses mails"

4.2.3 Des protocoles pour protéger son anonymat sur internet : VPN et Tor

Si le chiffrement des données permet qu'en cas d'interception, personne en dehors de vous et votre destinataire ne puissent lire vos données, on peut néanmoins bien souvent savoir que vous avez eu un échange avec telle personne (sans savoir ce que vous avez echangé comme informations). Afin d'empêcher cela, des services ont été inventés afin de garantir l'anonymat des échanges. Notamment les VPN et TOR

4.2.3.2 VPN

Afin de sécuriser notre anonymat sur internet, un sytème a été inventé, il s'agit du VPN (Virtual Private Network ou réseau privé virtuel). Pour résumer, il s'agit de passer par quelq'un·es d'autre pour faire transiter de façon chiffrée notre correspondance. Pour revenir sur l'exemple du courrier, c'est un peu comme si au lieu d'aller déposer votre courrier dans une boite aux lettres et de le récupérer dans la votre, vous demandiez à quelqu'un d'autre, qui fait ça de façon habituelle, de se charger de le faire à votre place. Du coup ce ne seront pas vos empreintes de doigts qui seront retrouvées sur la lettre mais les siennes. Pour résumer encore plus simplement, c'est un peu comme si vous utilisiez Fedex ou DHL à la place de LaPoste... mais vous pouvez aussi utiliser la PunkPost [2] ! En tous cas si La Poste ne peut plus lire vos échanges, l'intermédiaire (le VPN) lui le peut...

Du coup globalement le fournisseur de VPN c'est un peu le même problème. Votre fournisseur d'accès ne peut plus savoir ce que vous faites (à part que vous vous êtes connecté au VPN mais c'est tout) mais le fournisseur de VPN lui a accès à tout. Du coup, c'est une question de confiance. Est-ce que vous avez plus confiance en votre fournisseur VPN ou votre fournisseur d'accès. Est-ce que NordVPN (l'un des plus gros fournisseur de VPN privé du monde) a moins de chance qu'Orange de donner vos infos ? Et qui vous dit que dans le cas d'un fournisseur privé, il ne va pas utiliser vos infos pour les revendre à d'autre ?

Quelques opérateurs militants de confiance proposent néanmoins leurs services comme notamment Riseup.net, compatible avec ordinateurs et smartphones : https://riseup.net/fr/vpn. Après c'est comme la Punk Post, l'infrastructure n'étant pas gigantesque, elle n'est pas soutenue par des entreprises et gouvernements avec plein d'argent, donc c'est cool de les soutenir économiquement car c'est avec notre participation qu'elles existent et bien sur pensez à utiliser leurs services avec responsabilité. Faites un don ici : https://riseup.net/fr/don

4.2.3.1 Tor

Tor fonctionne différemment des VPN. Il utilise **un protocole dit en "onion"**. C'est à dire qu'il imbrique la connexion en plein de couches (comme les peaux d'un oignon, ou une poupée russe), on passe toujours par un circuit avec trois intermédiaires différents, et chacun "ouvre" sa propre couche sans pouvoir lire ce qu'il y a dans la couche du dessous.

Pour reprendre l'analogie avec les lettres, ça serait **comme si on mettait plein d'enveloppes fermées les unes dans les autres** et que trois facteur·ices différent·es distribuent et s'échangent ces lettres. Les facteur·ices peuvent ainsi uniquement savoir qui a ouvert l'enveloppe précédente, mais ne peuvent pas remonter à la première enveloppe ouverte. De même, la/le destinataire n'a aucune idée de qui a mis son enveloppe dans la grande enveloppe.

Pour en savoir plus sur Tor lisez l'article : "L'anonymat sur Internet grâce à la technique

du routage en oignon."

Attention, Tor n’est pas "magique" : des failles de sécurité sont régulièrement comblées. Rappelez vous, la sécurité garantie 1000% n’existe pas.. (Sauf bien sur si on chuchote dans l’oreille au milieu d’une forêt sauvage à notre meilleur pote de la vie)

4.3 Choisir les bons outils, une histoire de compromis

Comme on l’a déjà dit, l’outil parfait n’existe pas et la sécurité garantie 100% non plus. Choisir ses outils numériques, c’est donc une question de compromis. C’est au groupe qui va se réunir de décider de quel degré de confidentialité/facilité d’utilisation il a besoin.

Il faut bien évidemment aussi se poser les mêmes questions que lors d’une réunion physique avant de les utiliser.

4.3.1 Limite matérielle :

Pour prendre un exemple concret, il arrive que l’on juge qu’organiser une réunion dans un bar ne pose pas de problème de sécurité alors bien même que n’importe qui, en tendant l’oreille peut écouter nos conversations. Mais le groupe a décidé que le risque est mesuré car cela permet d’inviter des gens que l’on connaît un peu moins et on sait toutes et tous que ce ne sera pas l’endroit où seront transmis les plans secret de la cachette des dernières licornes ! Pour ce genre de cas, on préfèrera un rdv donné au dernier moment dans le Bunker de la forêt enchantée (que l’on aura passé au peigne fin pour vérifier qu’aucun micro/caméra n’a été installé dans les murs) !

En réalité, faute de Bunker dans la forêt enchantée, nos réunions les plus importantes ont lieu dans les espaces que l’on juge les plus sécurisés. En général, on se dit que les locaux dont on connait les personnes qui en possèdent les clés sont les plus sécurisés. Pourtant, un local syndical utilisé depuis 20 ans est il vraiment un lieu sécur ? Un squat où cohabitent 40 personnes qui laissent entrer tou·tes leurs "ami·es" est-il sécur ? Son appart qu’on a mis quelques fois en location sur AirBnB pour payer ses factures est-il secur ? Qui est vraiment cette personnne qui est venue installer la fibre chez nous ? Il ne s’agit pas de rentrer dans la paronoïa, simplement de se dire qu’en physique comme en ligne, penser maîtriser 100% de la sécurité est illusoire. Il faut faire des compromis si on ne veut pas s’organiser tout seul avec soi même.

Dans l’espace numérique, il est ainsi dit régulièrement qu’aucune communication sensible ne devrait passer par un téléphone portable. Les portables sont en effet plus facilement liés à une identité réelle et sont plus facilement piratables car à de rares exceptions près, une partie du matériel n’est pas libre, donc on ne sait pas vraiment ce qu’il y a dedans (que ça soit la puce wifi, la caméra ou souvent même le processeur qui est breveté). D’un autre côté utiliser le PC portable sous windows gracieusement prêté par votre entreprise afin de discuter avec vos collègues sur une possible grève est-il moins risqué ? De même pour communiquer avec quelqu’un·e n’ayant aucune notion de sécurité et encore moins d’informatique, mieux vaut-il lui faire installer Signal sur son smartphone [3] ou bien se

lancer dans une hasardeuse installation de clé de chiffrement mail GPG (sachant qu'il faudra déjà lui faire créer un nouvelle boite mail autre que Wanadoo.fr) ? A chaque situation, sa ou ses réponses. Il n'existe pas de réponse ni de contexte unique. L'important est de se poser les bonnes questions.

4.3.1 Se poser les bonnes questions

C'est donc à vous de réfléchir collectivement afin de choisir quels outils et quelles informations vont être partagé lors de votre réunion sur l'internet.
Voici quelques exemples de questions pour vous aider :

- Quelles informations sont sensibles ?
- De qui on se protège, de qui on se cache ?
- Quelles informations doivent être à tout prix cachées ?
- Quels seront les répercussions sur notre groupes si ces informations arrivent a d'autres ?

Par contre, il faut absolument éviter de se poser de fausses bonnes questions en terme de probabilité fictionnelle du type :

- En quoi mon groupe peut réelement nuire au intéret des méchants
- Quel est le ratio €uros dépensé/Gain réel pour les méchants
- Quel est le degrés de probabilité pour que je sois tracé

Il faut toujours partir du principe que nos communication peuvent être tracées !

5. Avantages et Inconvénients des logiciels les plus sécurisés

5.1 Tableau comparatif des différents logiciels de discussion utilisant internet

Vous le vouliez, c'est ce que vous attendiez depuis le début de ce @&#$! article ;) alors le voici, en exclusivité notre tableau comparatif des différentes solutions qui s'offrent à vous suivi de conseil sur ceux que nous avons testés pour vous (en fait pour nous au départ) en vraies conditions (d'où l'info Théorie/Pratique) :

Nom	Libre	Serveur/structure	Texte	Audio	Vidéo	Chiffrement	Anonymat Complet
Téléphone / SMS	non	Privé, Centralisé	2	1000	non	non	non (sauf achat en cash téléphone à usage unique)
Messenger / Instagram	non	Privé, Centralisé	150	50	50	non	non (sauf achat en cash téléphone à usage unique)

Nom	Libre	Serveur/structure	Texte	Audio	Vidéo	Chiffrement	Anonymat Complet
SnapChat	non	Privé, Centralisé	32	32	16	non	non (sauf achat en cash téléphone à usage unique)
Twitter	non	Privé, Centralisé	50	non	non	non	oui (en utilisant TorBrowser ou un VPN)
WhatsApp	non	Privé, Centralisé	256	4	4	oui	non (sauf achat en cash téléphone à usage unique)
Zoom	non	Privé, Centralisé	500	500	500	non	oui (uniquement par VPN)
Team	non	Privé, Centralisé	200	200	200	non	oui (uniquement par VPN)
Discord	non	Privé, Centralisé	200000	500	9	non	Non : impossible d’utiliser un VPN ou TorBrowser
Telegram	En partie	Privé, Centralisé	100000	2	2	non (oui uniquement en message secret)	non (sauf achat en cash téléphone à usage unique)
Signal	oui	Privé, Centralisé	200	2	2	oui, chiffrement complet EndToEnd	non (sauf achat en cash téléphone à usage unique)
Etherpad	oui	Autoheberg é, Centralisé	16	16	non	non (sauf CryptoPad)	oui (en utilisant TorBrowser ou un VPN)
Riot / Matrix	oui	Autoheberg é, Fédéré	illimité	16	16		oui (en utilisant TorBrowser ou un VPN)
Mattermost	oui	Autoheberg é, Centralisé	Illimité / 250 sur framasoft	non	non	non (mais le serveur peut être chiffré)	oui (en utilisant TorBrowser/Tor Soket ou un VPN)
Mumble	oui	Autoheberg	Illimité	200	non	oui mais il	oui (en utilisant

Nom	Libre	Serveur/structure	Texte	Audio	Vidéo	Chiffrement	Anonymat Complet
		é, Centralisé	théorique / 200 réel			faut en plus un serveur chiffré	TorSoket ou un VPN)
Jitsi	oui	Autohebergé, Centralisé	100 théorique, 50 pratique	50 théorique, 15 pratique	50 théorique, 5 pratique	oui mais il faut en plus un serveur chiffré	oui (en utilisant TorSoket ou un VPN)
Nexcloud Talk	oui	Autohebergé, Centralisé	12 théorique, 5 pratique	12 théorique, 5 pratique	non	oui, chiffrement complet EndToEnd	oui (en utilisant TorSoket ou un VPN)
XMPP / Jabber	oui	Autohebergé, Centralisé	illimité théorique	2	2	oui uniquement à 2 avec OTR activé	oui (en utilisant TorSoket ou un VPN)
IRC	oui	Autohebergé, Centralisé	illimité théorique	non	non	oui uniquement à 2 avec OTR activé	oui (en utilisant TorSoket ou un VPN)
Email + GPG	oui	Autohebergé, Fédéré	illimité sur une liste chiffré	non	non	oui, chiffrement complet EndToEnd	oui (en utilisant TorSoket ou un VPN)
Retroshare	oui	P2P	illimité théorique	non	non	oui, chiffrement complet EndToEnd	oui (en utilisant TorSoket ou un VPN)
Tox	oui	P2P	illimité théorique	2	2	oui, chiffrement complet EndToEnd	Oui, Tox fonctionne directement par TOR

5.2 Les logiciels libres que l’on recommande :

Mail Chiffré avec PGP (GPG) :

- *Avantage* : libre, fédéré, chiffrement le plus solide possible testé et approuvé, logiciel libre sur toutes les plateformes. Pour des échanges entre deux personnes nécéssitant le maximum de confidentialité, c’est l’outil le plus recommandé à

utiliser.

- *Inconvénient* : Nécessite l'utilisation d'un logiciel pour lire ses mails (Thunderbird avec le plugin d'Enigmail) , K9mail..) Si en suivant un tutoriel on peut sans trop de problème créer ses clés GPG pour échanger des mails entre 2 personnes, mettre en place une véritable liste mail entièrement chiffrée et complexe à mettre en place sans de solides connaisances informatiques.
- *Serveur conseillé* :
  - https://riseup.net /
  - https://www.autistici.org/services/mail
- *Tutoriel d'utilisation* :
  - https://riseup.net/fr/security/message-security/openpgp/best-practices
  - et aussi https://rebellyon.info/Comment-chiffrer-ses-mails

Signal (Texte) :

- *Avantage* : libre, ultra simple d'installation, chiffrement end to end, appels chiffrés entre deux personnes.
- *Inconvénient* : centralisé sur un serveur, les métadonnées passent par les serveurs d'Amazon, pas d'appel de groupe, limité à 200 personnes par groupe, nécessite un numero de téléphone, necessite un smartphone qui est donc potentiellement une faille, si une personne se fait arrêter, tout le groupe peut se faire choper. Gère mal les gros groupes.
- *Tutoriel d'utilisation* :
  - https://dijoncter.info/qu-est-ce-qu-on-connait-de-signal-1510
  - et aussi https://rebellyon.info/Comment-chiffre-ses-sms-sous

Etherpad (Texte)

- *Avantage* : Autohébergé, fonctionne avec TOr, aucune compétence technique n'est nécessaire, il faut ecrire directement c'est tout
- *Inconvénient* : en général pas chiffré, 16 personnes max, quasi inutilisable sur smartphone
- *Serveur conseillé* :
  - https://pad.riseup.net/
  - https://cryptpad.fr/
- *Tutoriel d'utilisation* : https://docs.framasoft.org/fr/etherpad/

JITSI (Texte, audio, video)

- *Avantage* : S'utilise avec un simple navigateur, sans inscription. Très simple à utiliser comme les pads. Conversation chiffrée
- *Inconvénient* : Prévu pour fonctionner pour 30 personnes, dépend en fait énormément du réseau internet, ne fonctionne pas vraiment au dessus de 10

personnes.
- *Conseil Sécurité* : Ne fonctionne pas avec TorBrowser mais fonctionne bien avec un VPN ou en passant par TorSoks. Sur smartphone, ne fonctionne pas avec un VPN mais fonctionne par Tor avec Orbot par le mode RPV.
- *Serveur conseillé* :
    - https://vc.autistici.org
    - https://meet.systemli.org/
    - https://meet.mayfirst.org/
- *Tutoriel d'utilisation* : https://docs.framasoft.org/fr/jitsimeet/

Mumble (uniquement audio)

- *Avantage* : Tres efficace, bonne qualité sonnore. Fonctionne bien même avec un vieil ordinateur et une mauvaise *connexion*. Application libre dispo sur toutes les plateformes PC et Smartphone.
- *Inconvénient* : Ne fonctionne pas vraiment dans un navigateur, il faut obligatoirement installer l'application (sur PC ou Smartphone). Pour passer par Tor il faut donc obligatoirement utiliser TorSoks (Sur Android Orbot par le mode RPV). Impossible de créer un nouveau salon avec un smartphone.
- *Serveurs conseillés* :
    - http://jntdndrgmfzgrnupgpm52xv2kwecq6mt4njyu2pzoenifsmiknxaasqd.onion
    - https://talk.systemli.org
    - https://mumble.mayfirst.org
    - https://mumble.libreops.cc
- *Tutoriel d'utilisation* : https://docs.framasoft.org/fr/jitsimeet/mumble.html

Mattermost (Texte) :

- *Avantage* : Autohébergé, application smartphone, nombre d'utilisateurs.rices illimités, fonctionne avec Tor
- *Inconvénient* : pas chiffré, pas d'appel vocal intégré, difficulté de s'autohéberger, Framateam qui propose le service le plus facile d'accès, est bloqué à 250 utilisateur.es, application smartphone qui ne se déconnecte pas automatiquement, pas de scroll infini dans l'historique ce qui complique les recherches. Pas de chiffrement bout à bout des conversations, le chiffrement reposant sur le chiffrement éventuel du disque dur du serveur. On se perd très vite dans les conversations si y'a un fort rythme de discussions -> l'outil "Répondre à", qui permet de faire des fils de discussion n'est presque jamais bien utilisé par tou-te-s, donc c'est vite le zbeul. Pas de possibilité de supprimer facilement et définitivement les messages.
- *Serveur conseillé* : Framateam (en utilisant Tor)
- *Tutoriel d'utilisation* : https://docs.framasoft.org/fr/mattermost/

MATRIX (riot/revolt) :

- *Avantage* : libre, fédéré, fontionne sous TOr/vpn, application smartphone, dépôt de linux, possible d'utiliser simplement le web browser sans rien à installer. Chiffrement des conversations, groupes illimités,..
- *Inconvenient* : pas d'appel dans les salles chiffrées, mais c'est possible de faire des appels de groupe
- *Tutoriel d'utilisation* : -**https://secoursrouge.org/dev/wp-content/uploads/2020/03/petitguidedesconfinees.pdf

XMPP/JABBER (Texte) :

- *Avantage* : Libre, chiffrement complet end to end, decentralisé, application libre sur toutes les plateformes
- *Inconvénient* : Ne fonctionne pas dans un navigateur, installation et configuration un peu compliquées, pas de conversation de groupe
- *Serveur conseillé* : https://riseup.net/fr/chat
- *Tutoriel d'utilisation* : https://rebellyon.info/Comment-securiser-ses-conversations

Nextcloud Talk (Texte, audio) :

- *Avantage* : libre, possibilité de se connecter avec des gens d'autres instances nextcloud (en fonction du serveur). Fonctionne dans un navigateur, logiciel multiplateforme, fonctionne avec TorSoks.
- *Inconvénient* : très peut de serveurs proposent ce services clé en main, il faut l'héberger soit même. Uniquement pour des petites groupes
- *Tutoriel d'utilisation* : https://docs.framasoft.org/fr/nextcloud/

IRC (Texte) :

- *Avantage* : Libre, application sur toutes les plateformes et dans un navigateur, chiffrement complet end-to-end pour des discussions à deux avec OTR
- *Inconvénient* : Pas de conversation de groupe chiffrée, chiffrement OTR n'est pas installé de base, interface en ligne de commande
- *Serveur conseillé* : https://chat.indymedia.org/
- *Tutoriel d'utilisation* : https://rebellyon.info/IRC-le-passe-et-l-avenir-de-la

On ne recommande pas, mais dans certaines situations cela peut quand même servir :

Conférence téléphonique (audio)

- *Avantage* : Pas besoin de connexion internet, ni d'ordinateur, ni smartphone, aucune compétence demandée, un simple téléphone suffit.

- *Inconvénient* : aucune sécurité, toutes vos conversations peuvent être écoutées et potentiellement stokées. Votre identité réelle est connue. On peut potentiellement utiliser un téléphone jetable pour un peu plus de sécurité mais n'utilisez ce système que si vous n'avez vraiment pas d'autre choix.
- *Serveur conseillé* : https://www.ovh.com/conferences (50 personnes max) / https://www.freeconferencecall.com/fr (1000 personnes max)
- *Tutoriel d'utilisation* : https://framasoft.frama.io/teletravail/#moins-de-10-personnes-a-reunir-utilisez-le-bon-vieux-telephone

Retroshare (Texte)

- *Avantage* : P2P (pas de serveur central), très bonne sécurité, chiffrement de groupe end to end avec GPG intégré
- *Inconvénient* : l'audio ne fonctionne pas, logiciel pas mis à jour depuis longtemps, très très moche, compliqué d'utilisation

Tox (Texte, Audio)

- *Avantage* : P2P (pas de serveur central), très bonne sécurité, chiffrement de groupe end to end avec GPG intégré
- *Inconvénient* : A la sortie de Tox, ce logiciel à été présenté comme THE super logiciel pour la sécurité. Sauf qu'on a découvert que la CIA y avait mis des portes dérobées pour écouter les conversations. Le logiciel à été totalement réecrit pour enlever ces portes cachées par la CIA. Pourtant, la confiance ayant été rompue, il n'y a pas grand monde dans la sécurité informatique qui conseille actuellement son utilisation.

Bonus : outils utiles

VPN

Pour utiliser le VPN de Riseup.net, rien de plus simple, rendez vous ici, tout est expliqué (attention cela fonctionne de manière aléatoire sous windows) : https://riseup.net/fr/vpn

TorBrowser

Pour installer TorBrowser, rendez vous ici : https://www.torproject.org/download/

TorSoket

- **Sur Debian/Ubuntu** dans un terminal, tapper : sudo apt install torsocks
- Lancer ensuite le logiciel de votre choix en ecrivant par exemple : "torsocks nomdevotrelogiciel" . Pour Mumble cela donne : torsocks mumble
- (on peut créer un raccourci sur le bureau pour lancer l'application avec Tor en un

clic)

Sur Android, installer "Orbot", tout en bas de l’application, à côté de "RPV de l’appareil entier", appuyer sur la roue crantée, choisissez les applications qui ont besoin de passer par Tor (Pumble, Jitsii Meet, Mattermost, Riot, ...). Faites ensuite glisser à droite le curseur "Mode RPV" en dessous à droite de l’onion, attendez un peu et quand l’onion sera vert, vous serez connecté. (Il arrive souvent que l’application ne fonctionne plus très bien au bout de plusieurs connexions/déconnexions, il faut forcer la fermeture de Orbot en allant sur l’icone, appuyer longtemps, chosir "informations sur l’application" puis "Forcer l’arrêt".

Sur Windows : Il n’existe pas d’application clé en main pour windows. Si vraiment vous n’avez pas le choix, vous pouvez suivre ce tutoriel assez compliqué : https://miloserdov.org/?p=2062 . Néanmoins, nous vous conseillons plutôt d’utiliser une clé linux Tails qui ne nécessite aucun "bidouillage" et risque même d’être plus rapide à mettre en place que ce tutoriel tout en vous garantissant une bien meilleure sécurité pour vous et vos correspondant·es.

Tails

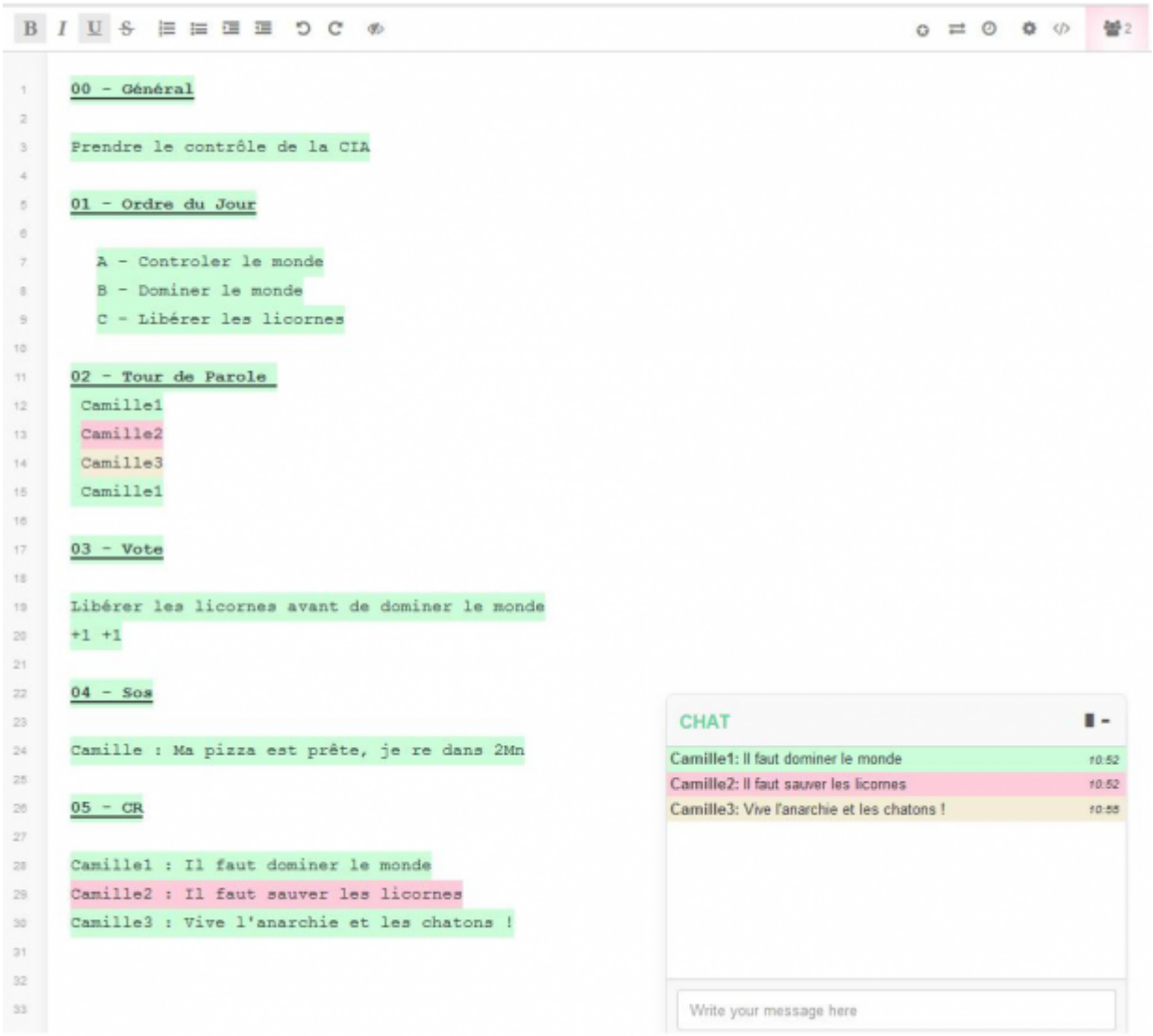
Tutoriel disponible ici : https://rebellyon.info/TuTORiel-Tails-21837

5.3 Adaptation

Normalement, à partir de ce tableau et de l’ensemble de l’article vous devriez sans problème pouvoir décider quel logiciel est le plus adapté à votre usage.

On peut par exemple avec un "simple" Etherpad (que tout le monde appelle "Les pads") organiser une très bonne et constructive réunion de 15 personnes.

Exemple :



Pour ajouter la conversation audio à ces mêmes 15 personnes, il suffit d’ouvrir une autre fenêtre du navigateur (plus pratique qu’un autre onglet) et de lancer une instance de Jitsi par exemple.

On peut aussi imaginer remplacer ce pad par Signal avec des groupes de conversations qui porteraient les mêmes noms.

Au dessus de 15, on peut toujours utiliser Signal mais pour l’audio passer sur Mumble (par exemple).

En fait on se rend compte que c’est pas terrible donc, on remplace Signal Desktop par Mattermost ou IRC (toujours avec Mumble).

A 200 sur Mattermost on trouve que ça va plus donc on remplace par Riot/Matrix ...

Un petit groupe à besoin de vidéo, on ajoute à Riot+Mumble, Jitsi pour une commission spécifique d’une grosse AG par exemple ...

Besoin de transmettre ensuite le compte-rendu de la réunion, on utilise une liste mail chiffré avec PGP !

Ce ne sont que des exemples, il vous appartient de tester les différentes combinaisons pour arriver à ce qui correspond le mieux à votre organisation !

Conclusion

Surtout, rappelez vous, c'est l'outil qui doit s'adapter à vos usages !
Surtout, protégez vous et n'oubliez pas qu'aucune sécurité n'est infaillible pour l'éternité !
Et enfin, pensez à bien fermer la porte à la Pookie dans le sas !

The_Mutu_Wire_Squad

Notes :

[1] la boîte qui permet de se connecter à internet

[2] Réseaux informels, où le principe est de donner un gros paquet de livres/K7 à un groupe de Punk qui fait une tournée musicale pour lui demander de déposer le paquet dans une des villes où il passera

[3] Lire quand même : infos pour bien utiliser signal