ChatGPT

Dossier complet pour la société fictive des « Anarcho-Geeks »

Ce dossier propose des outils pour un collectif imaginaire d'« anarcho-geeks » qui souhaitent explorer les potentiels de la *guerre informationnelle* sans violence. L'approche se veut expérimentale et joyeuse, mais s'appuie sur des principes d'autogestion, de créativité et de responsabilité. Les ressources ont été sélectionnées parmi des initiatives reconnues comme l'Electronic Frontier Foundation, Tactical Tech, Bellingcat et des travaux universitaires ou militants. Chaque partie vise à être accessible aux débutant·e·s tout en insufflant une culture hacker/anarchiste amusée et critique.

1. Kit d'atelier d'initiation sur une journée

Objectifs pédagogiques

1. **Comprendre les enjeux de l'information.** Les participant·e·s découvriront comment la circulation d'informations influence le pouvoir et pourquoi l'open source intelligence (OSINT) est une compétence accessible à tou·te·s. Bellingcat rappelle que la recherche open source est à la portée de quiconque dispose d'une connexion internet et d'un engagement suffisant [1].
2. **Acquérir des compétences en investigation et en vérification.** Exposing the Invisible propose des modules d'initiation à l'enquête citoyenne : recherche avancée, archivage de pages, géolocalisation, cartographie et évaluation de preuves [2]. L'objectif est d'apprendre à collecter et vérifier des informations de manière responsable.
3. **Explorer les tactiques créatives.** Les méthodes de Gene Sharp catégorisent les actions non violentes en protestations, non-coopération et interventions, avec des formes variées comme les slogans, les drapeaux, les actes symboliques ou les actions humoristiques [3]. L'atelier inclura du *culture jamming* (subvertir des messages publicitaires ou politiques) et des missions décentralisées inspirées du *hacking*.
4. **Renforcer la sécurité collective.** Selon l'Activist Handbook, les militant·e·s doivent modéliser leurs menaces pour déterminer ce qui doit être protégé, qui peut attaquer et quelles sont les capacités de l'adversaire [4]. L'atelier donnera des bases de sécurité numérique (chiffrement, VPN, gestion des mots de passe) et présentera des ressources comme la *Security In-a-Box* de Tactical Tech [5].

Programme horaire (indicatif pour une journée 9h00–17h00)

Heure	Activité	Description
9h00–9h30	**Ouverture horizontale**	Brise-glace collectif, définition des attentes et clarification de la règle d'or « ne pas nuire ». Chaque participant·e propose un pseudonyme pour favoriser l'anonymat.
9h30–10h30	**Intro à l'OSINT citoyen**	Présentation des méthodes de recherche open source. Bellingcat encourage à suivre des communautés et à apprendre via les réseaux sociaux [6]. Exemples d'exercices : trouver l'origine d'une photo via la recherche inversée, analyser les métadonnées d'une image.

Heure	Activité	Description
10h30–11h00	**Pause hacker**	Temps libre pour découvrir l'environnement (cafés, playlists pirates, etc.).
11h00–12h30	**Culture jamming et communication créative**	Découverte du *culture jamming*, qui détourne des symboles dominants pour dénoncer le consumérisme et l'injustice [7]. Atelier pratique : créer un visuel satirique à partir d'un logo. On invite l'utilisation de GIMP ou Inkscape.
12h30–13h30	**Déjeuner partagé (mode auberge espagnole)**	Chacun apporte un plat, discussion libre sur les pratiques d'autogestion.
13h30–14h30	**Mission décentralisée**	Répartition en petits groupes auto-gérés. Chaque groupe reçoit une mini-enquête (ex. : vérifier un fait viral, cartographier un réseau, créer un mème subversif). L'accent est mis sur la *mission command*, inspirée d'*Auftragstaktik* : donner un objectif clair et laisser une grande liberté de moyens [8].
14h30–15h30	**Initiation à la sécurité numérique**	Présentation des bases : chiffrement (comparé à une enveloppe scellée ou à une armoire verrouillée [9]), gestion des mots de passe, managers (KeePassXC), authentification à deux facteurs [10]. Les participant·e·s installent Privacy Badger, un VPN recommandé et configurent Signal.
15h30–16h00	**Pause & partage de ressources**	Présentation de la *Data Detox* et de la *Security In-a-Box* [11] [5].
16h00–17h00	**Restitution et autogestion**	Chaque groupe présente ses découvertes. Discussion sur la pertinence des tactiques humoristiques : selon le New Tactics, l'utilisation du rire aide à briser les tabous et la peur [12] et les cascades humoristiques peuvent servir de non-coopération efficace [13]. Débrief autour de la sécurité, de la responsabilité et des prochains pas.

Activités pratiques proposées

- **Recherches OSINT** : utiliser la recherche inversée d'images, les métadonnées, des outils de cartographie libre (OpenStreetMap) et l'archivage web pour vérifier une rumeur. Les modules d'Exposing the Invisible offrent des guides étape par étape [2].
- **Culture jamming** : détourner des logos ou des slogans pour questionner l'ordre dominant. ThoughtCo souligne que le *culture jamming* utilise des mèmes et des détournements pour dénoncer le consumérisme et l'exploitation [7].
- **Mission décentralisée** : se voir confier un objectif clair (par exemple cartographier les connexions d'un lobby) puis décider collectivement des moyens. L'autonomie est héritée de l'*Auftragstaktik* où le commandement donne l'intention et laisse les subalternes choisir la méthode [8].
- **Ateliers humoristiques** : créer une action symbolique non violente inspirée des « humorous political stunts » ; Sorensen définit ces interventions comme des performances qui utilisent l'humour pour exposer un discours dominant [14].

- **Sécurité numérique en pratique** : installation de Signal, prise en main de KeePassXC, configuration d'un VPN, utilisation de Privacy Badger et conseils pour créer des comptes anonymes via Tor lorsque les risques sont élevés [15].

Matériel requis (libre ou gratuit)

- **Ordinateurs portables ou tablettes** avec connexion internet. Préférer des systèmes libres (Linux) et navigateurs respectueux de la vie privée (Firefox, Tor). Le *Digital Enquirer Kit* propose des ressources sur le choix d'un VPN et des outils collaboratifs (CryptPad, Riseup Pad) [16].
- **Logiciels graphiques libres** : GIMP, Inkscape, Krita pour la création de mèmes et d'affiches. LibreOffice pour les documents.
- **Extensions de sécurité** : Privacy Badger, HTTPS Everywhere, uBlock Origin.
- **Messageries chiffrées** : Signal, Matrix/Element ; PGP via Mailvelope pour l'e-mail [17].
- **Matériel créatif** : papier, feutres, autocollants pour les activités hors ligne.
- **Documentation** : extraits imprimés des méthodes de non-violence de Gene Sharp [18] et du kit *Exposing the Invisible* [2].

Méthode d'animation

L'atelier privilégie l'autogestion et l'horizontalité : les facilitateur·ice·s proposent un cadre mais l'organisation interne est décidée collectivement. Chaque module s'ouvre par une courte introduction puis laisse place à des travaux en groupes auto-organisés. Le ton est décontracté et humoristique. Les participant·e·s sont encouragé·e·s à questionner, à apprendre en faisant et à partager leurs savoirs. La sécurité est une responsabilité collective : modéliser les menaces, protéger les personnes vulnérables et respecter la vie privée sont essentiels [4].

2. Micro-campagne de communication citoyenne

L'objectif est de sensibiliser le public à la puissance des outils d'enquête citoyenne et de l'humour dans la résistance non violente, tout en respectant la légalité.

Slogans et messages clefs

- **« Rire, enquêter, subvertir »** – un clin d'œil à l'usage du humour pour démystifier les pouvoirs. Le New Tactics souligne que l'humour brise les tabous et la peur [12].
- **« Hack the info, pas les gens »** – pour rappeler que l'objectif est de détourner l'information dominante, pas d'attaquer les individus.
- **« La vérité est open source »** – rappel que la recherche ouverte est accessible à tou·te·s [1] et peut renforcer la transparence.
- **« Crypto pour la liberté »** – écho au *Crypto Anarchist Manifesto* qui annonçait que le chiffrement permettrait des transactions anonymes et défierait le contrôle étatique [19].

Formats d'affiches ou visuels

- **Affiches A3 ou A4** avec slogans et illustrations satiriques. Utiliser des couleurs contrastées et des polices libres (Liberation Sans, DejaVu). Exemple : détourner un logo connu pour dénoncer la surveillance (p. ex. l'œil de Big Brother transformé en loupe).
- **Mèmes numériques** pour réseaux sociaux : images virales qui reprennent un schéma bien connu et y insèrent un message critique. ThoughtCo montre que le *culture jamming* utilise des mèmes basés sur des logos pour dénoncer des pratiques abusives [7].
- **Petits flyers** imprimables avec QR codes pointant vers des guides (Surveillance Self-Defense de l'EFF [20], *Data Detox* [11], *Exposing the Invisible* [2]).

- **Pochoirs** pour marquer des slogans sur des cartons ou des banderoles lors de manifestations, en restant dans la légalité.

Exemples de diffusion légale (offline/online)

- **Offline** : exposer les affiches dans les espaces associatifs, bibliothèques, cafés partenaires ; distribuer des flyers lors d'événements publics avec autorisation ; organiser des projections de documentaires sur l'OSINT.
- **Online** : publier les mèmes sur des comptes collectifs anonymisés ; utiliser des listes sur Twitter pour suivre et partager des ressources comme recommandé par Bellingcat [6] ; créer un blog statique (via Write.as ou GitHub Pages) contenant le manifeste et la fiche de survie. Attention : l'article de l'ICNC avertit que Facebook n'offre pas de réelle confidentialité et que les autorités peuvent surveiller les groupes [21]. Il faut évaluer les risques et éventuellement recourir à des pseudonymes ou à l'utilisation de Tor [15].

Outils libres recommandés

- **Inkscape** et **GIMP** pour les visuels et la mise en page.
- **Krita** pour l'illustration et la peinture numérique.
- **LibreOffice Draw** pour réaliser des flyers ou brochures.
- **Audacity** pour la production audio (podcasts), en respectant la légalité des contenus.
- **Freecad** ou **Blender** pour des projets 3D (ex. : impression de pochoirs).
- **Etherpad/CryptPad** pour l'écriture collaborative de communiqués (présenté dans le Digital Enquirer Kit [16]).

3. Mini-manifeste tactique et éthique

3.1 Relecture critique d'*Auftragstaktik* et de la « propaganda by the deed »

*L'*Auftragstaktik *est une méthode prussienne de commandement dans laquelle le commandant fixe des objectifs clairs puis laisse ses subalternes choisir comment les atteindre [8]. Les forces allemandes l'ont adaptée en « mission command » fondée sur l'intention du commandant, l'initiative disciplinée, les ordres de mission et la confiance mutuelle [22]. Pour notre collectif, l'idée est d'adopter l'autonomie de cette méthode (définir un but commun puis laisser chacun organiser son approche) tout en rejetant l'aspect hiérarchique et militaire. Une autogestion horizontale remplace les relations de commandement : chacun contribue selon ses talents, et la rotation des rôles évite la concentration de pouvoir.*

La « propaganda by the deed » désignait à l'origine des actions symboliques (violentes ou non) destinées à inspirer une révolte [23]. Certains anarchistes historiques ont privilégié l'exemple constructif : construire des institutions autogérées et préfigurer la société souhaitée. Nous rejetons les actions violentes et retenons la dimension symbolique et constructive : nos « actes » sont des enquêtes publiques, des créations artistiques et des expérimentations communautaires qui démontrent qu'une autre culture de l'information est possible.

3.2 Méthodes de résistance non violente et OSINT citoyen

- **Diversifier les tactiques** : Gene Sharp répertorie 198 méthodes, allant des slogans, chansons, boycotts, aux occupations non violentes [3]. Nos actions peuvent combiner ces tactiques avec des recherches open source et la satire. L'atelier propose ainsi de créer des mémoires collectives, de mener des micro-enquêtes et de produire des objets culturels.
- **Utiliser l'humour** : selon des analyses sur les mouvements non violents, les cascades humoristiques exposent et ridiculisent les discours dominants [13]. Le New Tactics raconte

comment le mouvement serbe Otpor! utilisait un tonneau représentant Milosevic pour inciter les passants à lui donner des coups, transformant la colère en rire [24]. L'humour réduit la peur et attire le public [12] ; Bruce Hartford souligne que le rire affaiblit l'autorité plus efficacement que la rage, car il désarme l'adversaire et attire les sympathisant·e·s [25].

- **Priorité à la sécurité** : Le guide *Surveillance Self-Defense* de l'EFF offre des bases pour comprendre la surveillance et choisir des outils adaptés [20]. L'ICNC rappelle que renoncer à la protection de la vie privée revient à se soumettre et que l'encryption protège les données en transit et au repos [9]. Il faut choisir des outils ouverts et auditables comme Signal, Mailvelope ou Veracrypt [17]. L'évaluation des menaces est contextuelle ; il s'agit d'identifier les adversaires, leurs capacités et les risques avant d'agir [4].
- **Responsabilité et légalité** : Les actions doivent respecter la loi et éviter de nuire. L'article sur Facebook souligne que les autorités peuvent accéder aux groupes et se servir des publications comme preuves [21] ; il est souvent préférable de recourir à des plateformes plus sûres ou d'utiliser des comptes séparés et anonymisés [15]. La diffusion de fausses informations ou l'atteinte à la réputation d'autrui est à proscrire ; les enquêtes doivent être vérifiées et les résultats partagés avec prudence, en suivant le principe « Do No Harm » mis en avant par le Digital Enquirer Kit [26].

3.3 Citations et inspirations

- **« Humor is the first step to break taboos and fears »** – Sami Gharbia [27]. Cette phrase rappelle que le rire est une arme pacifique contre la peur.
- **« Je suis un criminel. Mon crime est ma curiosité. [...] Vous vous moquez de nous, appelez-nous criminels. [...] Nous recherchons le savoir et vous nous appelez criminels. Nous cherchons l'illumination et vous nous appelez criminels. [...] Oui, je suis un criminel. Mon crime est celui de la curiosité. »** – *The Mentor*, *Hacker Manifesto*, 1986 [28]. Un appel à la liberté d'explorer et d'apprendre au-delà des frontières imposées.
- **« L'utilisation des consensus algorithm et des blockchains est en fait une solution anarchique à un problème de confiance »** – Tech Learning Collective [29]. Cette observation souligne comment les technologies décentralisées résonnent avec l'anarchisme.
- **« Les cryptographes ont découvert un moyen de permettre des transactions anonymes [...] qui permettra aux secrets d'être échangés librement et défiera le pouvoir des gouvernements [...] Les gouvernements tenteront de l'arrêter mais échoueront. »** – Timothy C. May, *Crypto Anarchist Manifesto* [19]. Cette prédiction invite à voir le chiffrement comme un outil d'autonomie.
- **« Ce que les hackers créent, ils ne le possèdent pas »** – extrait d'un *Hacker's Manifesto* de McKenzie Wark où il décrit la classe des hackers produisant des nouveautés sans maîtriser les moyens de production [30]. Cela rappelle l'importance de partager les connaissances et de lutter contre la privatisation de l'information.

4. Fiche de survie numérique (pour débutant·e·s)

Cette fiche vise à fournir des conseils simples et utilisables immédiatement. Chaque recommandation doit être adaptée selon le contexte et le niveau de risque.

4.1 Outils recommandés

Catégorie	Recommandations	Justification
Navigateurs	Utiliser **Firefox** avec les extensions **Privacy Badger**, **uBlock Origin** et **HTTPS Everywhere**. Pour l'anonymat, recourir à **Tor Browser**.	Les extensions limitent le pistage et sécurisent les communications. Le Tor Browser protège l'identité en masquant l'adresse IP et en routant le trafic via le réseau Tor.
Messageries	**Signal** pour les communications mobiles ; **Element/Matrix** pour des discussions en groupe ; **PGP/ Mailvelope** pour l'e-mail.	L'ICNC recommande des outils open source pour le chiffrement et cite Signal, PGP et Veracrypt comme exemples [17] .
VPN	Choisir un VPN reconnu et, si possible, à code source ouvert. Consultez les guides de l'EFF ou de la Freedom of the Press Foundation pour sélectionner un service.	Les VPN chiffrent le trafic et protègent contre l'espionnage sur des réseaux non sécurisés.
Gestionnaires de mots de passe	**KeePassXC** ou **Bitwarden**. Utiliser des mots de passe longs et uniques, et activer l'authentification à deux facteurs (2FA) [10] .	Les gestionnaires simplifient la création et le stockage de mots de passe robustes et protègent contre les vols de compte.
Stockage chiffré	**Veracrypt** pour chiffrer des dossiers ou des disques ; activer le chiffrement intégral (LUKS) sur Linux.	Le chiffrement protège les données au repos et empêche l'accès non autorisé [9] .
Collaboratif	**CryptPad**, **Riseup Pad** pour l'écriture collective ; **Nextcloud** pour le partage de fichiers.	Ces outils chiffrent les données et permettent une collaboration sans dépendre des grandes plateformes commerciales [16] .

4.2 Principes de base

- **Modéliser les menaces** : se poser les questions clés (« qui suis-je ? qui est mon adversaire ? que veut-il ? comment peut-il m'atteindre ? ») avant d'adopter des mesures de sécurité [4] .
- **Gérer ses mots de passe** : utiliser un gestionnaire, créer des phrases longues et uniques, ne jamais réutiliser un mot de passe. Activer la 2FA quand c'est possible [10] .
- **Mettre à jour** : maintenir son système et ses applications à jour pour bénéficier des correctifs de sécurité [31] .
- **Chiffrer ses données** : utiliser des outils d'encryption pour les données au repos (Veracrypt) et en transit (HTTPS, Signal) [9] .
- **Choisir sa plateforme** : éviter Facebook pour organiser des actions sensibles ; l'ICNC souligne que rien n'y est privé et que les autorités peuvent surveiller [21] . Préférer des plateformes plus sûres, ou créer des comptes anonymes via Tor [15] .
- **Limiter ses métadonnées** : désactiver la géolocalisation des photos, utiliser des pseudonymes pour l'activisme et séparer les identités publiques/privées.
- **Vérifier l'information** : appliquer la méthode scientifique en recoupant les sources, en vérifiant la date et l'origine, et en utilisant des outils d'OSINT pour confirmer ou infirmer une information [32] .

4.3 Conseils pour l'organisation de groupe

- **Autogestion et confiance** : adopter des structures horizontales et des rôles tournants pour éviter la centralisation du pouvoir. Inspirée de l'*Auftragstaktik*, la confiance entre membres prime sur la hiérarchie [8].
- **Canaux dédiés** : séparer les communications selon leur sensibilité (groupes Signal pour le sensible, listes de diffusion pour les annonces). Il est recommandé d'éviter les messageries publiques pour des sujets risqués [21].
- **Respect et humour** : maintenir un climat bienveillant et utiliser l'humour comme moyen de gestion des tensions. Selon Bruce Hartford, la satire et le rire sont plus efficaces que la rage pour mobiliser et désarmer les adversaires [25].
- **Formation continue** : organiser des ateliers réguliers pour mettre à jour les compétences OSINT, les pratiques de sécurité et les stratégies non violentes. Les guides *Exposing the Invisible* et *Security In-a-Box* sont de bonnes bases [2] [5].
- **Prendre soin les un·e·s des autres** : intégrer des moments de décompression, veiller au bien-être émotionnel et surveiller les signes de surmenage ou de paranoïa excessive. La sécurité doit être proportionnée aux risques réels [4].

Conclusion

Ce dossier montre qu'une exploration créative et responsable des potentiels de la « guerre informationnelle » peut s'inscrire dans une tradition de résistance non violente. En combinant l'OSINT citoyen, l'artivisme et l'humour, les « anarcho-geeks » peuvent exposer les abus, créer des imaginaires alternatifs et renforcer la culture de la sécurité. Les ressources open source citées ici – EFF, Tactical Tech, Bellingcat, ICNC – offrent des guides complets pour apprendre, s'organiser et protéger ses communications. Le défi est de maintenir un équilibre entre transparence et protection, audace et prudence, créativité et rigueur. Le rire et la curiosité restent nos meilleures armes.

---

[1] [6] First Steps to Getting Started in Open Source Research - bellingcat
https://www.bellingcat.com/resources/2021/11/09/first-steps-to-getting-started-in-open-source-research/

[2] Exposing the Invisible - The Kit — The Kit 1.0 documentation
https://kit.exposingtheinvisible.org/en/

[3] [18] 198 Methods of Nonviolent Action by Gene Sharp - The Commons
https://commonslibrary.org/198-methods-of-nonviolent-action/

[4] ICNC - Practitioners of Civil Resistance: Assess Your Cybersecurity through Threat Modeling
https://www.nonviolent-conflict.org/blog_post/practitioners-civil-resistance-assess-cybersecurity-threat-modeling/

[5] Security In-a-box
https://tacticaltech.org/projects/security-in-a-box/

[7] Culture Jamming - Definition and Examples
https://www.thoughtco.com/culture-jamming-3026194

[8] Auftragstaktik
https://nunosempere.com/blog/2023/11/30/auftragstaktik/

[9] [10] [17] ICNC - Deciphering Encryption, for Activists and Movement Allies
https://www.nonviolent-conflict.org/blog_post/deciphering-encryption-activists-movement-allies/

[11] Tactical Tech | Data Detox Kit – Libraries Stand for Privacy Participant Handbook
https://psu.pb.unizin.org/privacyliteracynatforum/chapter/data-detox-kit-tactical-tech/

12 24 27 Using Humor to Put an Oppressive Government in a Lose-Lose Situation - New Tactics
https://www.newtactics.org/tactics/using-humor-put-oppressive-government-lose-lose-situation/

13 14 Humorous Political Stunts: Nonviolent Public Challenges to Power - The Commons
https://commonslibrary.org/humorous-political-stunts-nonviolent-public-challenges-to-power/

15 21 ICNC - Facebook, Twitter, Telegram: Considerations for Activists and Organizers
https://www.nonviolent-conflict.org/blog_post/facebook-twitter-telegram-considerations-activists-organizers/

16 32 Verifying Online Information
https://digitalenquirer.org/en/verifying-online-information/

19 28 29 Anarchists on the Web · Anarchists on the Web · Omeka S at UVic Libraries
https://omekas.library.uvic.ca/s/anarchists/page/chronological

20 Electronic Frontier Foundation | Surveillance Self-Defense – Libraries Stand for Privacy Participant Handbook
https://psu.pb.unizin.org/privacyliteracynatforum/chapter/eff-ssd/

22 History, Mission Command, and the Auftragstaktik Infatuation
https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2022/Herrera/

23 Not protest but direct action: anarchism past and present - History & Policy
https://historyandpolicy.org/policy-papers/papers/not-protest-but-direct-action-anarchism-past-and-present/

25 Veterans of the Civil Rights Movement -- Audacity & Humor — Tactics of Nonviolence
https://www.crmvet.org/info/nvhumor.htm

26 Learn researching skills in these self-paced lessons!
https://digitalenquirer.org/

30 A Hacker's Manifesto | The Anarchist Library
https://theanarchistlibrary.org/library/mckenzie-wark-a-hacker-s-manifesto

31 Digital security for activists | Activist Handbook
https://activisthandbook.org/tools/security