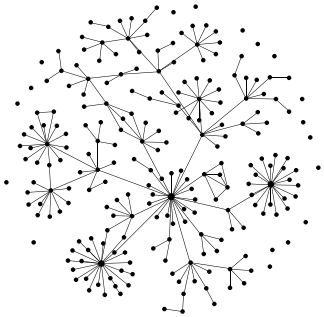
Alternet - Echapper à l'annexion de la vie privée
Lucas PIPARD - DSAA Design de produits - 2022
Pole supérieur de design - Villefontaine

Alternet

Echapper à l’annexion de la vie privée

Mémoire de recherche professionnel — Lucas Pipard

DSAA — 45°36'30.3"N 5°09'20.5"E — 2022



70 61 67

65 20 32

31 63 6f

6d 6d 65

6e 63 65

72 20 70

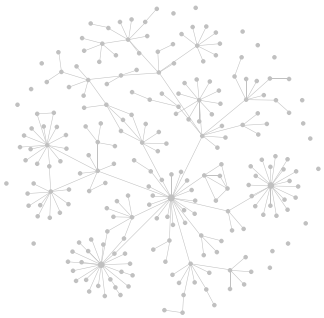
61 72 20

6c 61 20

Préserver sa vie privée à l'ère de l'exposition de soi est un acte révolutionnaire.

Alternet

Index



J'ai choisi de m'intéresser au fonctionnement de nos formes de communication au regard d'autres technologies passées comme émergentes car à mon sens, les services que nous utilisons aujourd'hui nous rattachent pour la plupart à des organisations privées et dans certains cas nous en rendent dépendant. A cette privation de choix s'adjoint la menace de la censure et des restrictions. Ce désir d'explorer des fonctionnements alternatifs ainsi que mon intérêt pour des technologies faisant infléchir ces mécanismes de monopole, tels que le P2P ou la blockchain, m'ont poussé à approfondir et à questionner la responsabilité du designer dans ce contexte et à rencontrer des communautés d'indépendants d'un monde discret ancré depuis longtemps dans un désir de liberté du net. Off-grid, chiffrement et autres crypto-monnaies ont toujours été soutenues par des personnes qui partagent l'envie de voir un monde plus libre par une autre approche de la gestion des données. Dans ce mémoire nous tenterons d'explorer ce filigrane du monde numérique qu'est l'Alternet.

IntroductionIntroductionIntroductionIntroductionIn
troductionIntroductionIntroductionIntroductionIntr
oductionIntroductionIntroductionIntroductionIntrod
uctionIntroductionI ntroductionIntroduc
tionIntroductionInt roductionIntroducti
on**Int**roductionIntro ductionIntroduction
IntroductionIntrodu ctionIntroductionIn
troductionIntroduct ionIntroductionIntr
oductionIntroductio nIntroductionIntrod
uctionIntroductionI ntroductionIntroduc
tionIntroductionInt roductionIntroducti
onIntroductionIntro ductionIntroduction
IntroductionIntrodu ctionIntroductionIn
troductionIntroduct ionIntroductionIntr
oductionIntroductio nIntroductionIntrod
uctionIntroductionI ntroductionInt**ro**duc
tionIntroductionInt roductionIntroducti
onIntroductionIntro ductionIntroduction
IntroductionIntrodu ctionIntroductionIn
troduction**I**ntroduct ionIntroductionIntr
oductionIntroductio nIntroductionIntrod
uctionIntroductionI ntroductionIntroduc
tionIntroductionInt roductionIntroducti
onIntroductionIntro ductionIntroduction
IntroductionIntrodu ctionIntroductionIn
troductionIntroduct ionIntroductionIntr
oductionIntroductio nIntroductionIntrod
uctionIntroductionI ntroductionIntroduc
tionIntroductionInt roductionIntroducti
onIntroductionIntro ductionIntroduction

0x49	0x76	0x75
0x75	0x6c	0x20
0x6a	0x6f	0x68
0x75	0x6a	0x6c
0x20	0x77	0x76
0x62	0x79	0x20
0x6b	0xc3	0xa9
0x6a	0x6f	0x70
0x6d	0x6d	0x79
0x6c	0x79	0x20
0x73	0x6c	0x20
0x7a	0x6c	0x6a
0x79	0x6c	0x61
0x20	0x6b	0x6c
0x20	0x6a	0x6c
0x20	0x74	0xc3
0xa9	0x74	0x76
0x70	0x79	0x6c
0x20	0x61	0x62
0x20	0x6b	0x6c
0x63	0x79	0x68
0x20	0x61	0x27
0x68	0x79	0x74
0x6c	0x79	0x20
0x6b	0x6c	0x20
0x77	0x68	0x61
0x70	0x6c	0x75
0x6a	0x6c	0x20
0x6c	0x61	0x20
0x6b	0x27	0x62
0x75	0x20	0x61
0x79	0x70	0x6b
0x6c	0x75	0x61

Introd**uc**ti**o**nIn**t**roductionIntroductionIntroductionIn
troductionIntroductionIntroductionIntroductionIntr
oductionIntroductionIntroductionIntroductionIn

Aujourd'hui, la quasi-totalité des services et objets que nous utilisons sont de près ou de loin rattachés à un acteur privé. On peut le voir dans l'actualité récente avec le scandale de l'affaire Pegasus, un logiciel espion commercialisé par NSO GROUP, spécialement conçu pour attaquer les deux systèmes d'exploitation téléphoniques les plus répandus, et mettre sous écoute des opposants politiques, des militants ou des journalistes. Le monopole d'utilisation détenus par ces services a ici constitué une faille et a permis la mise sous écoute de nombreuses personnes, faisant écho au scandale de Snowden et de la surveillance de masse de la NSA. Au travers de cette actualité se dessine l'un des risques que représente la centralisation dans l'usage de nos moyens de communication. Est-il vraiment pertinent de centraliser tous nos pouvoirs d'action entre les mains d'acteurs privés sous le prétexte d'une expérience d'usage plus fluide, créant une forme de facilité aliénante ?

Cette centralisation a fortement impacté nos usages et nos compétences techniques ces 20 dernières années et nous a rendu tributaires de grandes organisations ayant pour principal but la rentabilité avant même l'innovation. Cette dépendance se manifeste notamment par la perte progressive de nos connaissances techniques liées à ces services qui opère alors une véritable annexion sur nos usages numériques.

[1]Le monde - https://www.lemonde.fr/projet-pegasus/article/2021/07/19/projet-pegasus-comment-la-societe-israelienne-nso-group-a-revolutionne-l-espionnage_6088692_6088648.html

Une annexion dans le sens ou notre environnement numérique quotidien est investi par des acteurs divers, souvent inconnus, tel une forme d'annexion de notre territoire privées. Pour être en mesure de fonctionner, ces services envahissent nos vies privée, et cette annexion se manifeste par une perte progressive d'autonomie. De ce fait, nous nous exposons au risque de la censure, des restrictions ou de la surveillance, que ces acteurs peuvent décider d'implémenter quand bon leur semble.

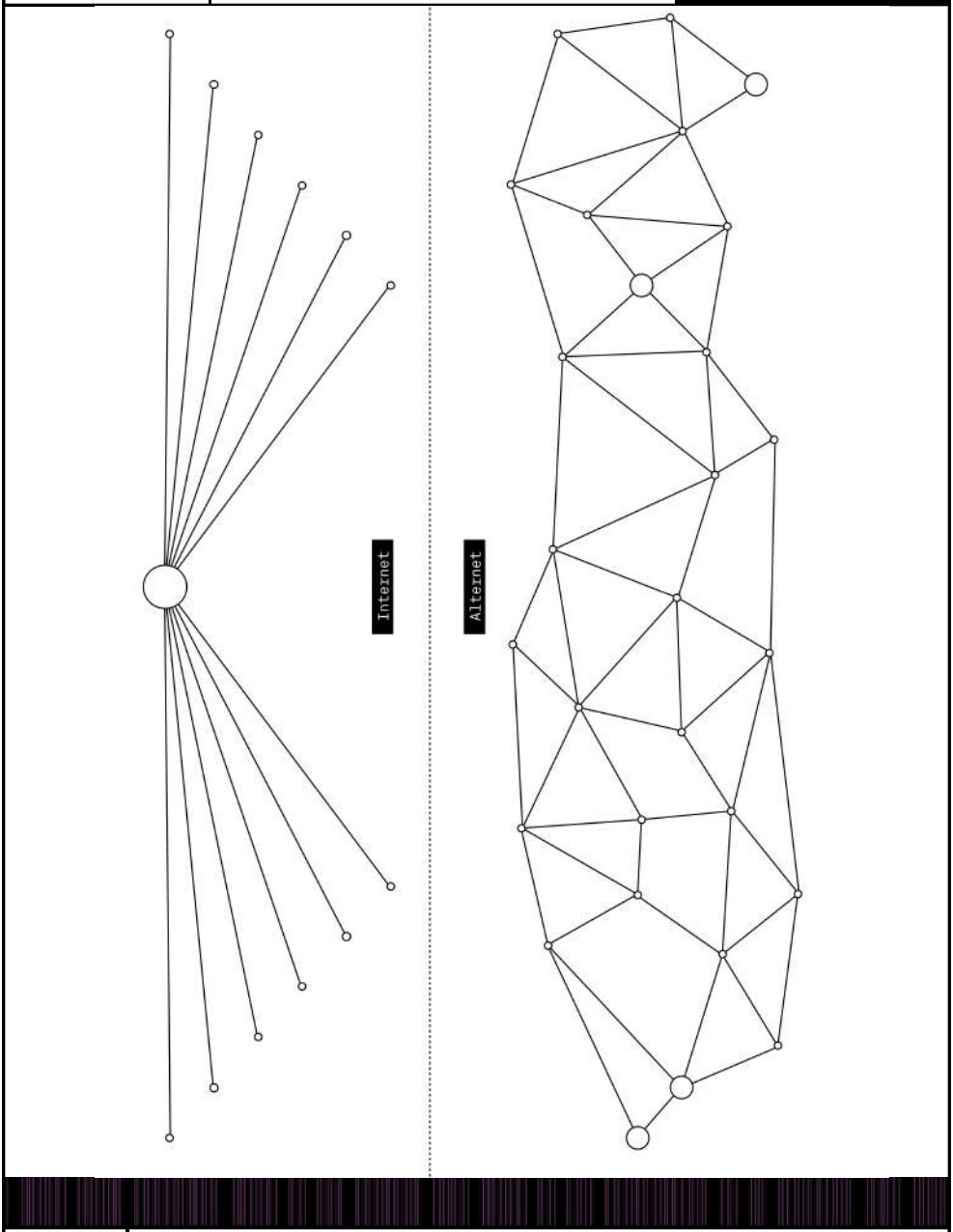
En réponse à ce système prônant la transparence du “rien à cacher”, de nombreuses initiatives émergent sous la forme d'une contre-culture sous-jacente qui utilise le réseau de manière détournée. Tel un point opaque dans un système transparent, ces communautés utilisent le web d'une manière différente, plus discrète et cryptique, à des fins diverses.

C'est pourquoi dans ce mémoire, nous etudier **en quoi ces initiatives alternatives sont une forme de lutte contre l’annexion de la vie privée ?**

Pour ce faire, dans un premier temps nous allons voir comment une collecte systématique de tous les aspects de notre comportement a été mise en place progressivement. Nous nous attarderons sur les influences historiques qui ont forgés la tendance de contrôle sécuritaire de nos télécommunications et identifierons les mécanismes de design qui permettent une telle annexion. Dans un second temps nous verrons comment des initiatives indépendantes essayent de construire une échappatoire au travers de ce que nous allons appeler *Alternet*. Ayant une construction et un fonctionement parfois différent des usages du grand public en accord avec un forme de furtivité, nous essayerons de décortiquer ces codes pour mieux les comprendre.

L'utilisateur moyen paye le web au prix fort; il abdique sa vie privée, sa liberté, son indépendance pour une dose régulière de narcissisme[2]

[2]Le mystère Satoshi : enquête sur l'inventeur du bitcoin - Rémi Forte 2021



Pastebin

Schema personnel

Une mise en place progressive au fil de l'histoire

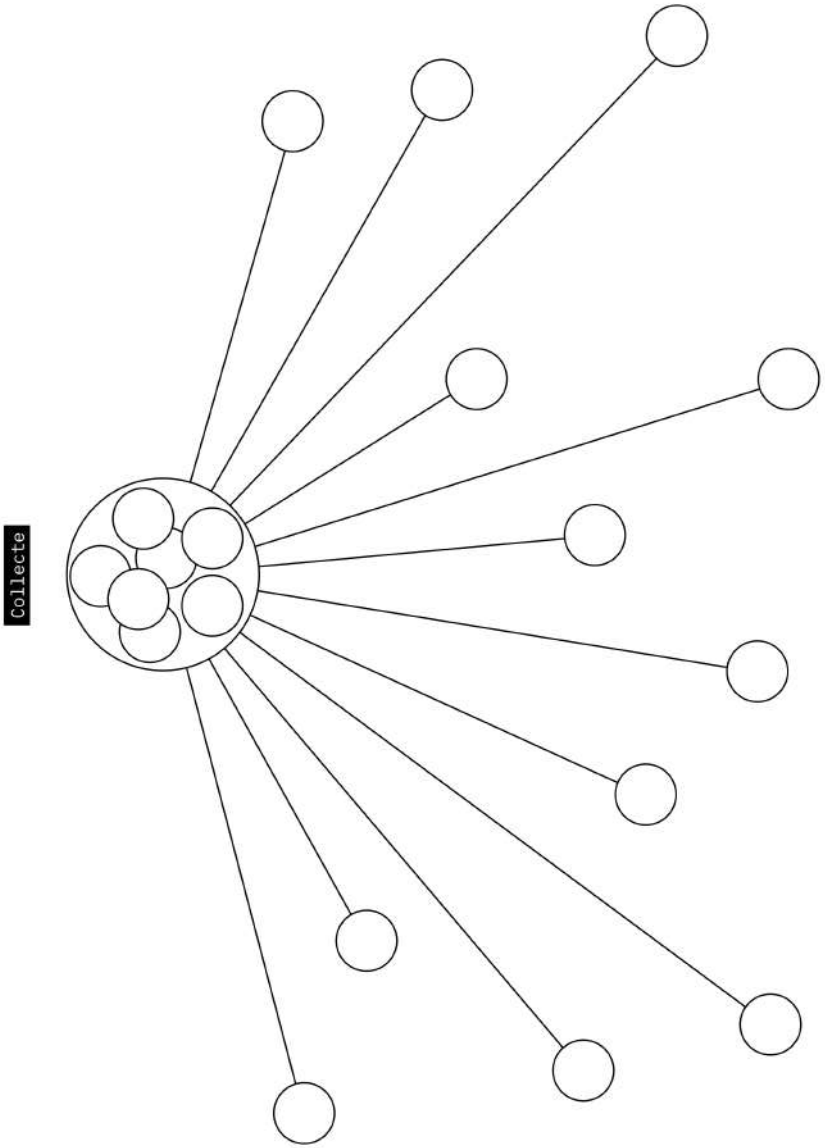
UnProblèmeInhérentANosTechnologiesUnProblèmeInhérentAN
osTechnologiesUnProblèmeInhérentANosTechnologies**s**UnProb
lème**In**hérentANosTechnologiesUnProblèmeInhérentANosTech
nologiesUnProblèmeInhérentANosTechnologiesUnProblèmeIn
hérentANosTechnologiesUnProblèmeInhérentANosTechnologi
esUnProblèmeInhérentANosTechnologiesUnProblèmeInhérent
ANosTechnol ologiesUnPr
oblèmeInhér érentANosTe
chnologiesU sUnProblème
InhérentANo NosTechnolo
giesUnProbl blèmeInhére
ntANosTechn nologiesUn
ProblèmeInh hérentANos
Technologie iesUnProblè
meInhérentANosTechnologiesUnProblèmeInhérentANosTechno
logiesUnProblèmeInhérentANosTechnologiesUnProblèmeInhé
rentANosTechnologiesUnProblèmeInhérentANosTechnologies
UnProblèmeInhérentANosTechnologiesUnProblèmeInhérentAN
osTechnologiesUnProblèmeInhérentANosTechnologiesUnProb
lèmeInhérentANosTechnologiesUnProblèmeInhérentANosTech
nologiesUnProblèmeInhérentAN**os**TechnologiesUnProblèmeIn
hérentANosTechnologiesUnProblèmeInhérentANosTechnologi
esUnProblèmeInhérentANosTechnologiesUnProblèmeInhérent
ANosTechnologiesUnProblèmeInhérentANosTechnologiesUnPr
oblèmeInhérentANosTechnologiesUnProblèmeInhérentANosTe
chnologiesUnProblèmeInhérentANosTechnologiesUnProblème
InhérentANosTechnologiesUnProblèmeInhérentANosTechnolo
giesUnProblèmeInhérentANosTechnologiesUnProblèmeInhére
ntANosTechnologiesUnProblèmeInhérentANosTechnologiesUn
ProblèmeInhérentANosTechnologiesUnProblèmeInhérentANos
TechnologiesUnProblèmeInhérentANosTechnologiesUnProblè
meInhérentANosTechnologiesUnProblèmeInhérentANosTechno
logiesUnProblèmeInhérentANosTechnologiesUnProblèmeInhé
rentANosTechnologiesUnProblèmeInhérentANosTechnologies
UnProblèmeInhérentANosTechnologiesUnProblèmeInhérentAN
osTechnologiesUnProblèmeInhérentANosTechnologiesUnProb
lèmeInhérentANosTechnologiesUnProblèmeInhérent**ANoN**

68	61	67	65	20	c3	aa	66	71	65	20	65
67	64	20	78	6d	20	6e	61	7a	7a	71	20
68	61	75	71	2c	20	76	27	71	65	62	c3
a8	64	71	20	63	67	71	20	58	6d	20	72
75	7a	4d	78	75	66	c3	a9	20	7a	71	20
68	61	67	65	20	70	c3	a9	6f	71	68	64
6d	20	62	6d	65	2c	20	79	6d	75	65	20
76	71	20	78	6d	75	65	65	71	20	c3	a7
6d	20	6d	67	20	74	6d	4c	4d	44	70	2e

1_Un problème inhérent à nos technologies

Nous vivons à un instant T dans le temps, et sur certains thèmes, notre vision a tendance à obscurcir ce qu'il s'est passé en dehors de cette perspective. Dans le cas de la vie privée, il est facile de ne voir que son état actuel sans point de référence antérieur. En ce qui concerne la gestion de la vie privée et sa potentielle annexion par des tiers, il est important de la replacer dans le contexte de son évolution en réaction à des événements socio-culturels. En effet, depuis que des technologies de communication existent, celles-ci sont utilisées en vue de recolter et d'accumuler des informations sur les individus, dans le but d'avoir un avantage stratégique sur eux. La problématique de la collecte et du stockage de toutes formes d'informations personnelles semble être nouvelle mais est en réalité bien plus ancienne. Au fil de l'histoire, cette collecte d'informations (photographies, historiques de délit) a pour principale fonction la lutte contre le crime, ou s'effectue à des fins administratives au travers de registres de recenssement. Cependant, des problemes de censure et de controle des informations échangées peut déja se manifester sous la forme de l'interception des courriers des soldats pendant la guerre par exemple. C'est avec des technlogies toujours plus rapides et des distances de communicatios toujours plus étendues que le potentiel d'interception des messages devient véritablement problématique. Cependant avec l'évolution des ces technologies de transmission dans un contexte historique tendu, les finalités de ces logiques de collectes prennent une dimension controversable.

1_Un problème inhérent à nos technologies



Pastebin

Schema personnel

2_Point de bascule vers une intensification

La guerre froide, les affaires d'espionnage et le wiretapping ont intensifié les enjeux autour de la protection de la vie privée. Le wiretapping, pouvant être traduit par "mise sous écoute", consiste à se brancher sur les lignes téléphoniques de quelqu'un afin d'espionner et d'enregistrer ses communications. Cette méthode utilisée d'abord par des détectives privés puis par le gouvernement pose déjà des questions sur l'éthique de telles pratiques illégales utilisées par les forces de l'ordre, à l'instar de ce débat télévisé du Washington Spotlight de 1954 :*"l'État s'engagerait alors dans une forme de conduite illégale violant la vie privée des habitants. Et l'État n'est en aucun cas en mesure de l'imposer"*[3]. Ici la mise sous écoute d'un individu présumé suspect, motivée par le maccarthysme, induit la généralisation de cette pratique à tous les citoyens, tous potentiellement suspects. C'est pourquoi, dès les années 50, on voit fleurir des communautés qui tentent de se placer en opposition à ces potentielles menaces de surveillance.

Les Phreakers, ou les radio pirates en sont un bon exemple, car ces regroupements d'individus détournent des dispositifs pour leurs usages particuliers, ou leurs libertés.

[3]Do we Need Wiretapping Laws? (1954) - https://www.youtube.com/watch?v=IWsWWjFS0No

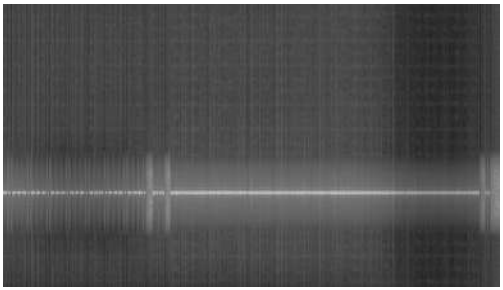
2_Point de bascule vers une intensification

Pastebin

Schema personnel

Ces communautés utilisant les ondes de manière détournée se basent sur les échanges chiffrés entre des pays pendant la seconde guerre mondiale, et utilisent encore aujourd'hui la radio ShortWave qui ne nécéssite aucuns antenne relais pour fonctionner. En effet, les signaux émis rebondissent sur la ionosphère permettant une écoute à l'échelle mondiale. Encore aujour'hui des number stations[4] émettent des messages chiffrés et cryptiques dont le récepteur est inconnu, et le seul à pouvoir en décrypter la signification. Communautés indépendantes ou espions communiquants avec leurs pays d'origine, tout le monde peut écouter le message, mais seuls ceux à qui il s'adresse peuvent le comprendre.

Exemple de Number Station que j'ai enregistré et converti pour au final ne pas être capable de déchiffrer le message.



[4]Priyom, forum communautaire d'écoute, d'enristrement et de documentation des number station. https://priyom.org/about
Exemple de number station : https://priyom.org/media/152427/s06.ogg

Cependant, ces communautés n'ont pas suffi à enrayer l'évolution de la surveillance. C'est ainsi que différentes affaires d'espionnage voient le jour, tels que le COINTELPRO ou le scandale du Watergate. L'évolution des modes de transmission toujours plus rapides et distants se poursuit et la menace de la surveillance plane toujours en arrière plan. Avec l'accélération des modes de communication, les informations importantes sont de plus en plus sur le même plan que l'insignifiant. Nous passons progressivement à ce qui est décrit comme des modes de communication de masse par Yves Citton, dénonçant alors la confusion entre vérité et pertinence[5]. Jean Baudillard évoque également "un vertige de la réalité" pour dénoncer une forme de boulimie grandissante, transformant le quotidien et l'information en "consommables"[6]. Ce phénomène est en premier lieu exploité par le marketing et pour la vente d'informations dans les médias traditionnels, jusqu'au tournant des attentats du 11 septembre 2001 où tout s'accélère. À partir de cet incident s'installe une doctrine sécuritaire, ouvrant une nouvelle ère de la collecte massive des données personnelles, au nom de la lutte contre le terrorisme. On peut parler de réelle annexion ici, puisqu'en parallèle de ces événements, les réseaux sociaux et internet sont en plein essort, et des masses de données tirées du comportement de chacun sont générées, prêtes à être exploitées par des tiers au travers d'algorythmes toujours plus perfectionnés pour prédire notre comportement.

[5]Yves Citton. « Médiarchie », pp. 939-340, citant Günther Anders, L'Obsolescence de l'homme p. 151, 155-156.
[6]Jean Baudrillard, La société de consommation, 1970, page 32-33.

2_Identifier les mécasimes de design qui portent atteinte aux données personnelles

IdentifierLesMécasimesDeDesignQuiPortentAtteinteAu**x**Don
néesPersonnellesIdentifierLesMécasimesDeDesignQuiPorte
ntAtteinteAuxDonnéesPersonnellesIdenti**fi**erLesMécasimes
DeDesignQuiPortentAtteinteAuxDonnéesPersonnellesIdenti
fierLesMécasimes inteAuxDonnéesPe
rsonnellesIdenti gnQuiPortentAtte
inteAuxDonnéesPe sMécasimesDeDesi
gnQuiPortentAtte llesIdentifierLe
sMécasimesDeDesi xDonnéesPersonne
llesIdentifierLe ortentAtteinteAu
xDonnéesPersonne imesDeDesignQuiP
ortentAtteinteAu entifierLesMécas
imesDeDesignQuiP esPersonnellesId
entifierLesMécas AtteinteAuxDonné
esPersonnellesId DesignQuiPortent
AtteinteAuxDonné erLesMécasimesDe
DesignQuiPortent onnellesIdentifi
erLesMécasimesDe teAuxDonnéesPers
onnellesIdentifi QuiPortentAttein
teAuxDonnéesPers écasimesDeDesign
QuiPortentAtteinteAuxDonnéesPersonnellesIdentifierLesM
écasimesDeDesignQuiPortentAtteinteAuxDonnéesPersonnell
esIdentifierLesMécasimesDeDesignQuiPortentAtteinteAuxD
onnéesPersonnellesIdentifierLesMécasimesDeDesignQuiPor
tentAtteinteAuxDonnéesPersonnellesIdentifierLesMécasim
esDeDesignQuiPortentAtteinteAuxDonnéesPersonnellesIden
tifierLesMécasimesDeDesignQuiPortentAtteinteAuxDo**n**nées
Per**s**onn**ell**esIdentifierLesMécasimesDeDesignQuiPortentAt
teinteAuxDonnéesPersonnellesIdentifierL**esM**écasimesDeDe
signQuiPortentAtteinteAuxDonnéesPersonnellesIdentifier
LesMécasimesDeDesignQuiPortentAtteinteAuxDonnéesPerson
nellesIdentifierLesMécasimesDeDesignQuiPortentAtteinte
AuxDonnéesPersonnellesIdentifierLesMécasimesDeDesignQu
iPortentAtteinteAuxDonnéesPersonnellesIdentifierLesMéc
asimesDeDesignQuiPortentAtteinteAuxDonnéesPersonnelles
IdentifierLesMécasimesDeDesignQuiPortentAtteinteAu

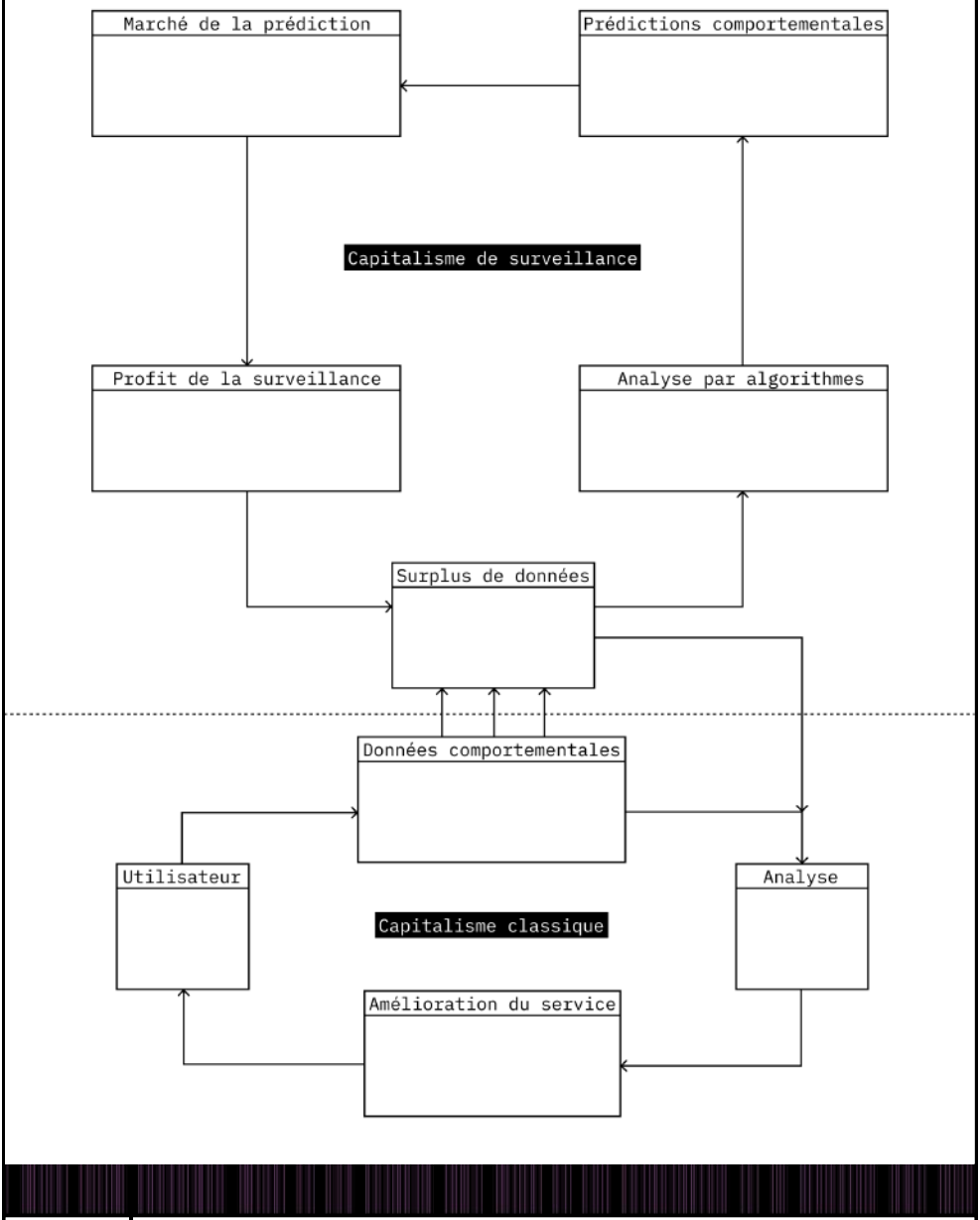
0x43	0x65	0x20	0x6e	0x27
0x65	0x73	0x74	0x20	0x70
0x61	0x73	0x20	0x61	0x75
0x73	0x73	0x69	0x20	0x73
0x69	0x6d	0x70	0x6c	0x65
0x20	0x71	0x75	0x65	0x20
0xc3	0xa7	0x61	0x20	0x64
0xc3	0xa9	0x73	0x6f	0x6c
0xc3	0xa9	0x20	0x69	0x6c
0x20	0x76	0x61	0x20	0x66
0x61	0x6c	0x6c	0x6f	0x69
0x72	0x20	0x63	0x68	0x65
0x72	0x63	0x68	0x65	0x72
0x20	0x61	0x76	0x65	0x63
0x20	0x70	0x6c	0x75	0x73
0x20	0x2a	0x70	0x72	0x6f
0x66	0x6f	0x6e	0x64	0x2a

1_Nouvelle forme de capitalisme

L'incident du 11 septembre a provoqué l'intensification des logiques de surveillance dans la société. La collecte et l'analyse des données à grande échelle permet le recenssement global des multiples aspects de notre comportement. C'est la surveillance couplée à la génération d'un très grand nombre de données qui mène alors à l'émergence d'un nouveau systeme économique et politique, décrit par Shoshana Zuboff comme le *Capitalisme de Surveillance*. Dans son livre *The Age of Capitalism Surveillance: The Fight for a Human Future at the New Frontier of Power*[7], l'autrice décrit ce phénomène comme une nouvelle étape dans le capitalisme, qui vient utiliser l'individu comme matière première pour son profit, au travers de l'annexion de ses données. Ses données comportementales sont générées par l'utilisateur d'un service sans même qu'il soit averti ou rémunéré, puis elles sont réinvesties dans l'amélioration ou le financement du service. Cette dimension d'analyse constante des données implique une génération en continu de données par l'individu, permise grâce à l'ancrage toujours plus important des services fonctionnants sur ce principe dans nos vies.

[7]Shoshana Zuboff, The Age of Capitalism Surveillance: The Fight for a Human Future at the New Frontier of Power, page 92 a 97.

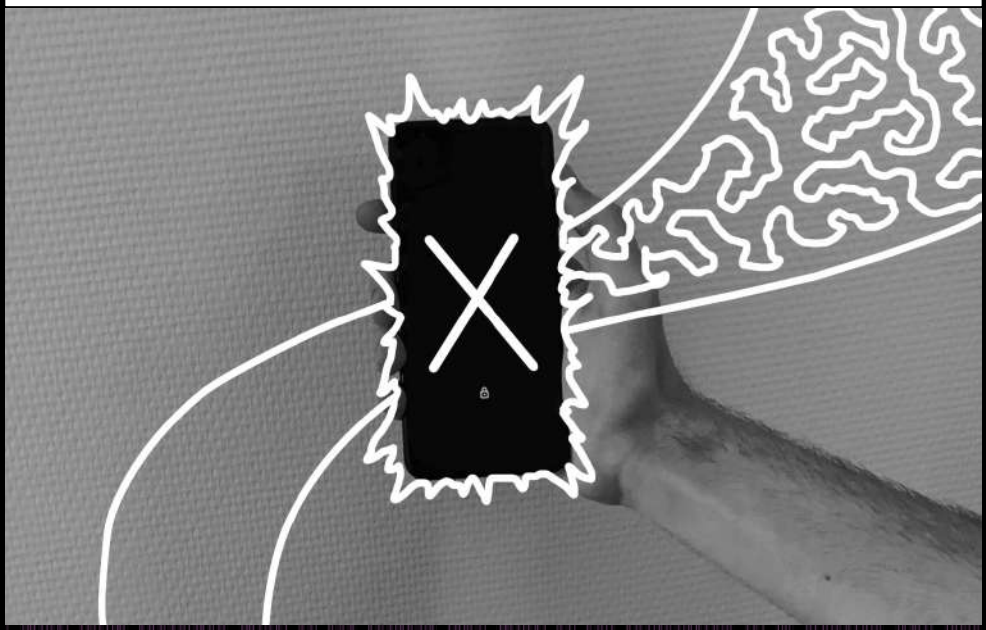
1_Nouvelle forme de capitalisme



[7]Shoshana Zuboff, The Age of Capitalism Surveillance: The Fight for a Human Future at the New Frontier of Power, page 92 a 97. Schéma reformulé.

1_Nouvelle forme de capitalisme

Pour témoigner de la puissante intrication du capitalisme de surveillance dans nos vies, j'ai mené une expérimentation sur ma propre utilisation, en essayant de supprimer Google de mon téléphone depuis un an. Ainsi le 8 mars 2021 à 19h26, je décide de "détourner" mon Pixel 3a pour supprimer toute connexion avec son constructeur: Google. Les conclusions après un an d'utilisation sont alarmantes. Malgré avoir supprimé Google de mon smartphone et même supprimé la possibilité de se connecter à Google, ses services réussissent tout de même à s'infiltrer dans mon utilisation, en se rendant indispensables pour interagir avec certaines structures comme l'école ou d'autres professionnels.



Pastebin

Photographie personelle

Cette intrusion est rendue particulièrement visible par les manques qu'elle génère, un peu comme une addiction. Au final, ce service a simplement pris plus d'importance à d'autres endroits de mon utilisation, passant plus par mon ordinateur que par mon smartphone et jouant sur la dépendance de mon environnement à leurs services.

Ce constat témoigne de la stratégie sous-jacente de ces modèles de services centralisés : améliorer la fluidité et la facilité d'utilisation de leurs services pour se rendre indispensables dans un usage quotidien. Nous en sommes réduits à devoir faire des concessions sur nos usages si l'on refuse d'utiliser ce service, en nous privant ainsi de fonctionnalités devenues aujourd'hui essentielles. Notamment avec ce design de la fluidité, sans connaissance technique nécessaire pour l'usager, une dépendance se crée au sein des usages personnels comme professionnels. Par ailleurs cette dépendance est articulée à une perte d'autonomie technique et s'inscrit dans une logique qui alimente le capitalisme de surveillance.

1_Nouvelle forme de capitalisme

1_Nouvelle forme de capitalisme

Organisation du téléphone.

Ecran de verrouillage	Ecran d'accueil	Applications	Isolement avec shelter
Peu de distraction	**épure**	**Profil personnel**	**Profil professionnel**
Pour éviter les distractions, seules l'heure et les notifications de signal sont activées et les autres ne fonctionnent pas.	Une forme d'épure avec une tendance au tout noir pour maximiser le temps de batterie et minimiser la lumière bleue.	Ici j'utilise un maximum d'App alternatives pour essayer de préserver mes données d'une exploitation par des companies.	Grace à Shelter, je peux isoler des applications dans une "machine virtuelle" isolée du reste de mon téléphone.

Cette démarche est en quelque sorte une lutte contre l'annexion et s'ancre dans une forme minimalisme digital.

Le principe peut etre résumé comme tel :"si je n'ai pas de données, elles ne peuvent pas etre exploitées."

La limite reste la meme : Comment réduire la génération de données sans etre synonyme de retour en arrière

2_Prédiction via des données implicites

Il est important de souligner le caractère positif de ce modèle, qui est la gratuité apparente de l'accès aux services. On ne doit rien payer pour l'utilisation du service qui se rémunère et s'améliore grâce aux données générées de manière implicite. Cependant la gratuité prétendue de ces services se paye autrement, avec une monnaie plus bien personnelle : notre comportement.

Vendue à des partis politiques, des publicitaires, des sociétés inconnues aux noms obscurs, cette ressource est la plus précieuse, au point qu'elle est parfois surnommée la "nouvelle essence"(the new oil) dans certains domaines pour souligner sa profitabilité. De plus, il est important de comprendre que ce n'est pas directement via nos actions que ce profit est généré, mais par la génération de données annexes, des "métadonnées", que notre comportement est déduit et croisé avec les métadonnées de notre entourage, pour cerner nos moindres faits et gestes.

2_Prédiction via des données implicites

Pour essayer de comprendre comment ces données implicites sont générées, j'ai réalisé une expérimentation, ayant l'apparence d'un simple atelier d'écriture. Les volontaires se sont alors inscrits sans même demander les tenants et aboutissants de l'expérience au sein de laquelle ils s'engageaient, de la même manière que lors d'une inscription sur un réseau social. Mais cet atelier cache en réalité une récolte et une analyse de leurs données. J'ai constitué deux groupes, un ayant des donneés préremplies et l'autre non, comme détaillé sur l'annexe 2.

Le but est en fait de voir leurs réactions et de générer une discussion, de laquelle je tire des traits de comportement, des alignements politiques, des avis etc. J'ai ensuite aggloméré ces données pour former des typologies de personnes, essayant de jouer le rôle de la prédiction comportementale à une moindre échelle. L'étape finale est la création de fiches résumant une orientation politique globale des participants, qui est un produit qu'ils n'ont en aucun cas voulu générer mais qui a tout de même été effectué tacitement.

2_Prédiction via des données implicites

Protocole de l'atelier :

1_Recrutement

Recruter des participants dans 2 groupes avec une consigne vague. Ils s'engagent sans connaitre les aboutissants exacts.

Groupe 1	Groupe 2
Cihan x	Léa y
Coraline x	Charlie y
Nastassia x	Christelle y
...	...

2_Recherche données privées

Constitution de fiches d'entretiens préremplies ou vierges pour constater leurs réactions à une annexion de données.

compilation d'informations via internet

3_Interview et débat

Conduite d'un interview prétexte a la génération d'un débat. Prise de note de leur comportement durant le débat.

Génération **implicite** de données comportementales

4_Analyse comportemental

Analyse des éléments du comportement et création d'un score en fonction d'un bareme de réticence a l'annexion de données.

Attribution d'un score de complaisance

Pastebin

Schéma personnel

2_Prédiction via des données implicites

Atelier écriture fictive	Document ex0000003
Date d'attribution	16/11/2021 09:41
Date de restitution	23/ /2021
	Numéro 02/700

Numéro d'identification	141131
Nom	[redacted]
Prénom	[redacted]
Naissance	[redacted]
Adresse	[redacted]
Localisation	[redacted]
Contacts	[redacted]

Demande	Décrivez un monde ou toutes les communications seraient publiques et consultables par n'importe qui

Un monde ou toutes les communications soient publiques et consultables ?
Les messages pourraient être contrôlés sur une plateforme (un site, une appli ?) et tout le monde y aurait accès, pour consulter la vie intime des gens, leurs rapports sociaux !
On aurait plus rien à cacher à personne, plus de secrets, le monde ne serait alors que transparence ? Si internet et les réseaux ont poussé à un tel paroxysme le partage des données et l'hyper accessibilité, peut-être que l'écriture manuelle, les lettres seuls alors un moyen de conserver une part d'intimité dans nos échanges. Un réseau secret, sans fil pourrait se mettre en place. Face à cette sensation de curiosité intrusive ? Cependant, cette ouverture sur les données de tous pourraient peut-être faciliter le travail des médecins, des autorités, ... Auraient-elles un contrôle sur nos actions ? Simplement un droit de regard et une classification ?

Mots-clefs	INTIMITÉ – CONSÉCRATION – HYPER ACCESSIBILITÉ – RÉSEAU SECRET – CURIOSITÉ – FACILITER TRAVAIL ÉTAT

Invalide si recouvert [redacted]

Pastebin

Schéma personnel

2_Prédiction via des données implicites

Fiche éxaminateur	Document ex0000003ex
Date d'attribution	16/11/2021 09:41
Date de restitution	23/11/2021
Numéro	/700

[redacted]

Notes comportementales	[redacted]

COMMENT? TOUT ÇA?/ CHOQUÉ / (PK?) NUMÉRO OK? | OUAIS → POURQUOI J'AURAI REMPLI ADMINISTRATION

→ UN PEU ÉTRANGE / JE VOIS PAS EN QUOI ?

→ QUELQU'UN L'A FAIT POUR MOI ? WTF ?

LES PRÉNOMS SONT CRITIQUES / HYPER OFFICIELS | CURIEUSE COMMENT

→ PERTURBANT / ADRESSE FLIPPANT CERCLE SOCIAL / FAMILLE.

NUMÉRO PAS CHOQUANT.

→ DOCUMENTS APPART → PLEINS D'INFOS / ÉCOLE / PAPIERS AIDES

→ ON DONNE CAR ON A ENVIE ALORS ON SE POSE PAS LA QUESTION

→ PAS MOI ALORS BIZARRE. | JE NE SUIS PAS LECTEURE INITIALE.

→ FLIPPANT : GROUPE SANGUIN / INFO TRÈS PRÉCISE.

GLOBALEMENT OFFUSQUÉE DES INFOS PRÉREMPLIES CAR CE N'EST PAS ELLE QUI LES A DONNÉS!

INFORMATION CRITIQUE = ADRESSE DES PARENTS / PRÉNOMS. ACT.

→ MODIFICATION DES RAPPORT SOCIAUX

RS = TOUTE NOTRE VIE

PLUS DE SECRET

→ TROP DE TRANSPARENCE

→ RÉSEAUX SECRETS INTIMES / LETTRES LOW TECH. DÉCLONOVIA

→ ÉCRITURE MATÉRIELLE = INTIME / PRIVATE.

ÉCRITURE IMMATÉRIELLE = LIBRE / PUBLIC

→ CHANGEMENT BRUSQUE / → RÉVOLTE

→ PROGRESSIF → OK, ASSIMILÉ, NOUVEAUX RAPPORTS SOCIAUX

→ FACILITE POLICE / MÉDECINE

→ DROIT DE REGARD → POURQUOI ? → QU'EST CE QU'ON EN FAIT ?

CONFLIT ENTRE LIBERTÉ / VIE PRIVÉE.

Mots-clefs

Invalide si recouvert

Pastebin	

Schéma personnel

2_Prédiction via des données implicites

Fiche éxaminateur	Document ex0000003ev	
Numéro d'identification	141131	
Date de restitution	26/11/2021 11:54	Numéro 02/700

Atribution des scores	
Naissance - non rempli	
Adresse - non rempli	
Contact - non rempli	
Rétissance- refus	
Mention Chine	
Mention NSA/FBI	
Mention Darknet	
Mention surveillance	-5
Mention Black Mirror	
Surpris - pas surpris	+10
Information critique	-5
Sensibilisé privacy	+15
Inscris sur réseaux	+20
Rempli régulièrement	
Utilise fausses infos	
Dystopique - Utopique	+10
Mention epistolaire	-10
Mention Prison	
Mention Espionnage	
Vocabulaire fataliste	
Vocabualaire péjoratif	-5
Vocabulaire mélioratif	
Mention médicale	+5
Mention Familliale	-10
Accepte enregistrement	+5

Complaisant

Valeur totale de complaisance	**35**

Invalide si recouvert

Pastebin

Schéma personnel

2_Prédiction via des données implicites

Les répercussions de la récolte des données sur nos vies sont nombreuses, allant de la prédiction de notre comportement et de nos pensées pour provoquer un acte d'achat, à l'exploitation politique à des fins de traffic d'influences comme avec le scandale de Cambridge Analytica. Dans le cas de cette affaire, la collecte et l'analyse méticuleuse a constitué une arme politique qui a permis d'exercer une forte influence sur les choix de nombreuses personnes. Dans une étude de l'université polytechnique de St.Petersbourg, il est mis en évidence que c'est le vide juridique qui entoure l'usage des données personnelles d'utilisateurs par des sociétés privées qui a permis une telle exploitation.

Ici les données générées en masse de manière implicite par les utilisateurs ont constitué une base de données exploitables à leur propres influence sur leurs prises de décision. On peut dire que les utilisateurs ont généré leurs propres produits, dans le sens où ils sont eux même le carburant nécessaire au fonctionnement de leur propre fil d'actualité. Dans ce contexte, la citation d'Edward Snowden prend tout son sens : "***Businesses that make money by collecting and selling detailed records of private lives were once plainly described as "surveillance companies." Their rebranding as "social media" is the most successful deception since the Department of War became the Department of Defense***[8]."

[8]Twitter - Edward Snowden https://twitter.com/Snowden/status/975147858096742405?ref_src=twsrc%5Etfw - 17 mars 2018

2_Prédiction via des données implicites

On constate donc une discordance entre un discours des réseaux sociaux et plus globalement de la politique du 21ème siècle basée sur la transparence et le "je n'ai rien à cacher" et le fonctionnement interne très opaque de ces entreprises à des fins de dissimulation des mécanismes de captation de la vie privée. Ce paradoxe et l'opacité de ces mécanismes internes pour toute personne non experte, mêlés au vide juridique qui entoure l'exploitation des données[2] peuvent être perçus comme les moteurs d'un modèle économique malsain basé sur l'instrumentalisation de l'individu.

Mais dans ce cas, à quel degré le designer participe-t-il à ce mécanisme ? Dans un sens, il vient renforcer les usages décrits précédement en répondant à un désir de fluidité qui peut servir des motivations bien plus larges. Cependant, il se trouve dans une zone de gris. Il souhaite une meilleure expérience pour les utilisateurs mais évolue au sein de systèmes aux principes arbitraires à des buts de rentabilité, n'étant au final en rien bénéfique pour les utilisateurs.

[2]RGDP, loi du 25 mai 2018 en europe, RGDP, https://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/es/pdf

Avec cette position ambigüe, le designer est coincé entre des impératifs de rentabilité et le désir d'amélioration de service des utilisateurs, souvent trop peu sensibilisés aux problématiques de souveraineté des données. Mais dans cette zone de gris, où l'on veut garder un usage fluide tout en évitant l'annexion des données, certains ce sont improvisés designers, inventeurs, programmeurs, en essayant de produire leurs propres alternatives. À défault d'être reconnus comme tels par un systeme ne répondant plus qu'à ses propres desseins, certains ont décidé de se servir par eux mêmes, pour creer des services qui correspondent à leurs valeurs.

“Préserver sa vie privée a l'air de l'exposition de soi c'est un acte révolutionnaire”

[10]Le mystère Satoshi : enquête sur l'inventeur du bitcoin - Rémi Forte 2021

Devenir furtif

68	61	67	65	20	c3	aa	66	71	65	20	65
67	64	20	78	6d	20	6e	61	7a	7a	71	20
68	61	75	71	2c	20	76	27	71	65	62	c3
a8	64	71	20	63	67	71	20	58	6d	20	72
75	7a	4d	78	75	66	c3	a9	20	7a	71	20
68	61	67	65	20	70	c3	a9	6f	71	68	64
6d	20	62	6d	65	2c	20	79	6d	75	65	20
76	71	20	78	6d	75	65	65	71	20	c3	a7
6d	20	6d	67	20	74	6d	4c	4d	44	70	2e

```
grVCVyg/ud3xckVcMb+1KA==
UauH8rFibUAkmAsUHkvW6g==
tk6KJ/AZQ9fcGUSqFUPwdg==
AgW+3Qh+FhETutiKWzsnLg==
d3Lr3b7LI/RAHVEMRAuPIw==
1RwiirhH3yEigmu8ECXEeQ==
kKl04DHynYMfGmWBagXf6w==
??????
```

1_La furtivité comme dénominateur commun des alternatives

Nous avons vu que la culture des alternatives a commencé très tôt avec les radio pirates et la communauté des Phreakers dans les années 50, mais on constate de manière plus globale l'apparition de contre-cultures au fil du temps, en réaction à des problématiques de surveillance toujours plus marquées. C'est avec l'acces au chiffrement qui assure un dégré supérieur d'intimité et de furtivité que les premières initiatives individuelles émergent peu à peu.

La furtivité intervient vite comme une notion importante, marque de fabrique des alternatives, permettant de passer sous les radars de la surveillance et de l'analyse comportementale. À l'image de l'ouvrage de science fiction *Les Furtifs*[11] de Alain Damasio, qui décrit une société entièrement privatisée ou le refus d'assimilation à la technologie et à la surveillance induit d'être un furtif, vivant dans les interstices de la société, ces initiatives utilisent la furtivité pour s'extraire du systeme, loin de la vue des utilisateurs peu expérimentés et des usages centralisés. Dans son œuvre de fiction, Alain Damasio conceptualise la furtivité comme un outil physique et virtuel indispensable pour évoluer en dehors des regards, au point que si un furtif est vu, il meurt.

[11] Les furtifs - Alain Damasio

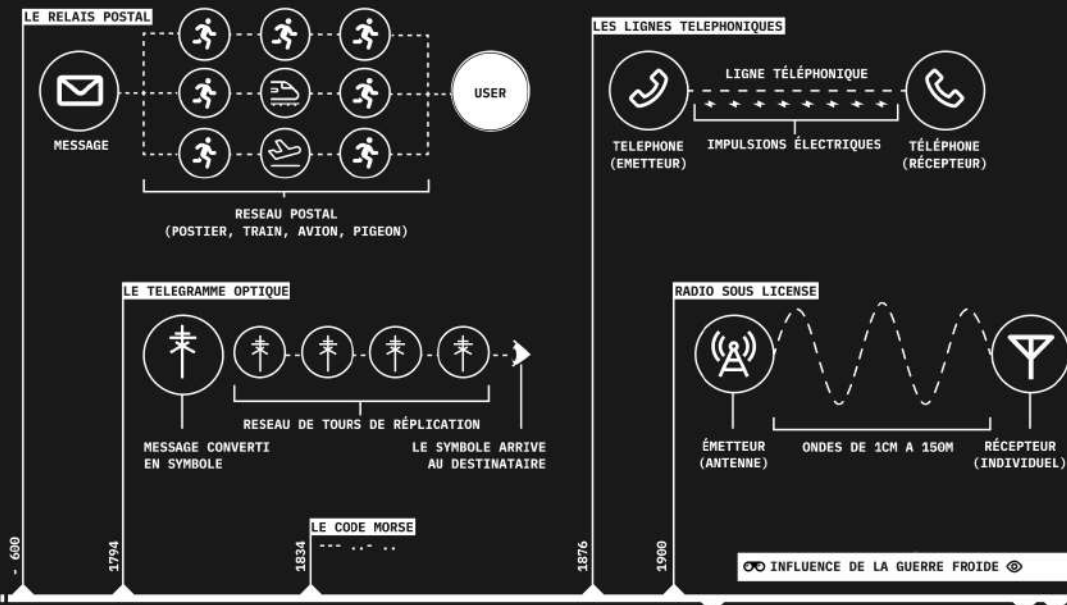
1_La furtivité comme dénominateur commun des alternatives

Damasio exprime une version exacerbée de notre réalité actuelle, où la surveillance est encore plus banalisée qu'à présent et où l'hyperconnectivité à des services privés a peu a peu fait perdre leurs pouvoir d'actions aux États, rendant les méga-corporations seuls maîtres à bord. Cette futivité vitale face à des sociétés géantes et sans visage se retrouve dans certaines initiatives indépendantes ayant pour but de ne jamais se faire remarquer pour se préserver d'une d'attention néfaste qui parasiterait leur fonctionnement, voire pire, intéresserait les méga-corporations pour un éventuel rachat.

Le basculement dans le monde contemporain va faire naître une nouvelle forme de résistance, grâce à la démocratisation d'internet. Les cypherpunks, un groupe de programmeurs activistes, prônant le chiffrement comme droit universel, vient consolider les bases d'une contre-culture numérique naissante.

Dans cette frise chronologique j'ai replacé l'émergence de cultures alternatives en réactions a des phénomènes sociaux et politiques, ayants un impact sur les technologies de communication.

TIMELINE DES MODES DE TRANSMISSIONS



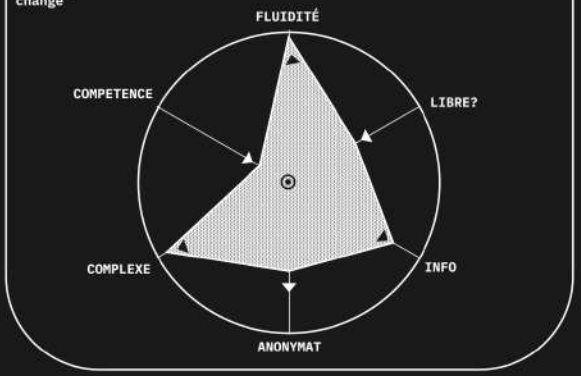
RESSENTI DU PUBLIC

Pensez-vous qu'internet est libre ?	"libre bof; moins qu'on le pense"
Ressentez-vous un changement d'internet ?	"Les restrictions augmentent"
Vos communiactions sont plus libre qu'avant ?	"non mais il y en a plus"
Vous essayez de lutter contre ça ?	"pas vraiment;pas assez renseigné"

"Nos usages se sont multipliés et fluidifié c'est bien plus facile"

"Tout nous fait croire qu'on est plus libre; mais le fonctionnemment fait l'inverse"

"Je ne sais pas si internet à évolué mais mon usage à lui bcp changé"



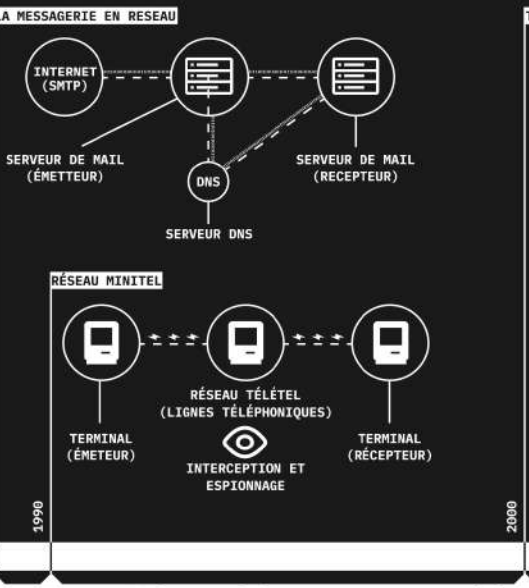
1939 — MOUVEMENT CYPHERPUNK — 1955 — 1960

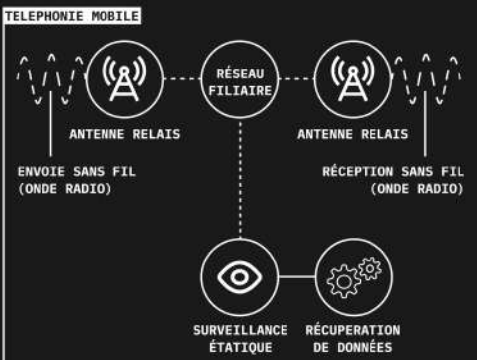
MISSING FILE
JUDE MILHON
INVENTE LE TERME
DE CYPHERPUNK

LES RADIOS PIRATES

COURANT PHREAKER

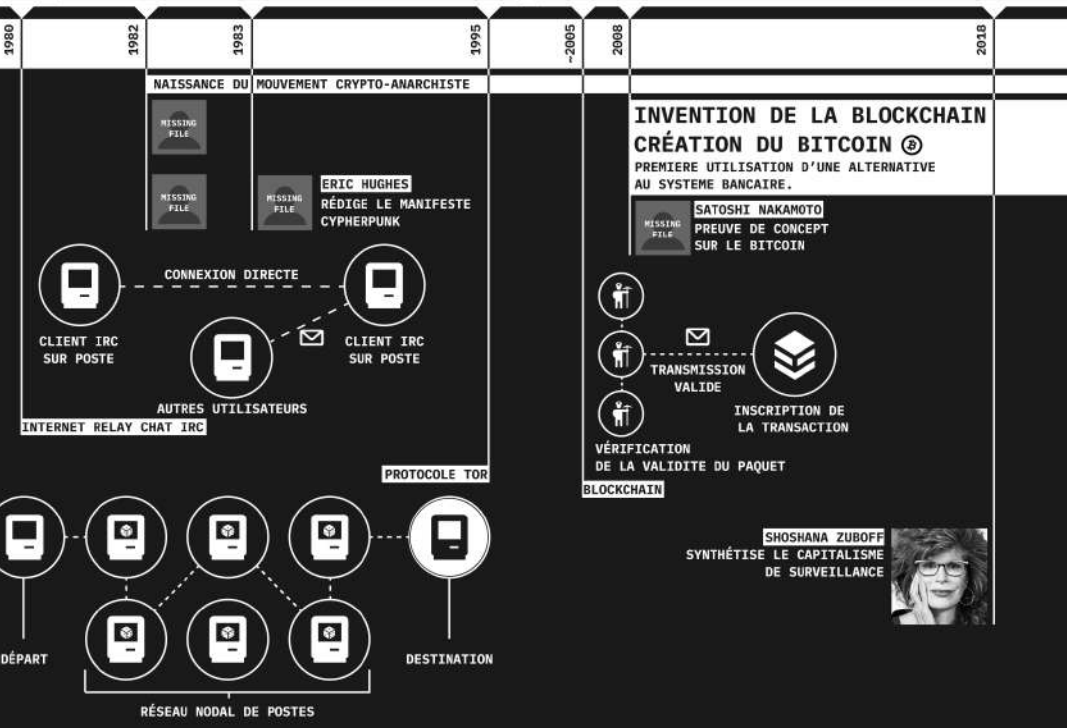
MISSING FILE | MISSING FILE | MISSING FILE | MISSING FILE





"J'AI L'IMPRESSION QUE À CAUSE DE LA MASSE D'INFOS QUI CIRCULE ON EST OBLIGÉS DE DÉPENDRE DE GROSSES SOCIETÉS ALORS QUE C'EST PEUT-ÊTRE PAS LE CAS"

INFLUENCE DU 11 SEPTEMBRE



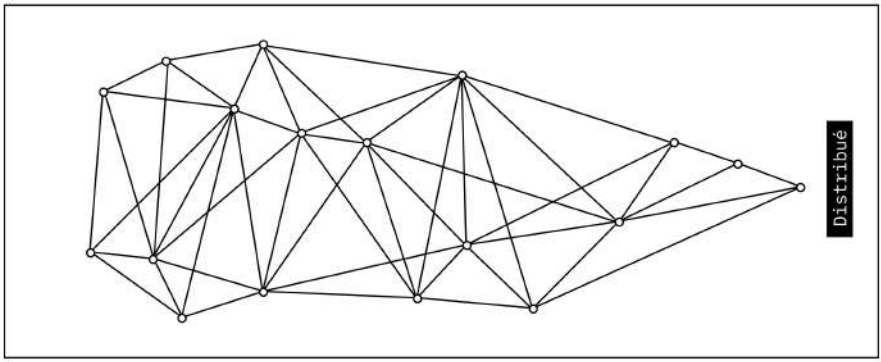
1_La furtivité comme dénominateur commun des alternatives

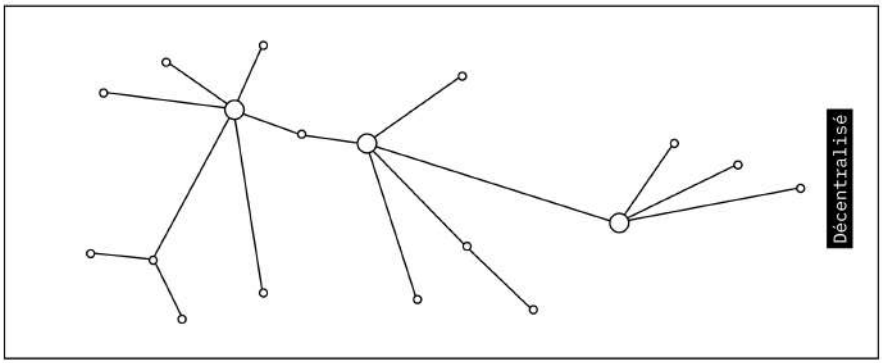
Dans le manifeste Cypherpunk, Eric Hughes écrit "*Nous ne pouvons attendre des gouvernements, des entreprises et des autres organisations majeures et sans visage de nous accorder une vie privée par acte de bienveillance...Nous devons défendre notre vie privée par nous-mêmes si nous nous attendons à en avoir une. Nous devons nous rassembler et créer des systèmes qui nous permettent d'arriver à des échanges anonymes*[12]." Les cypherpunks expriment alors le besoin grandissant de furtivité dans les échanges et les communications, à une époque ou internet perd peu à peu sa dimension d'espace anonyme pour se transformer progressivement en une machinerie commerciale.

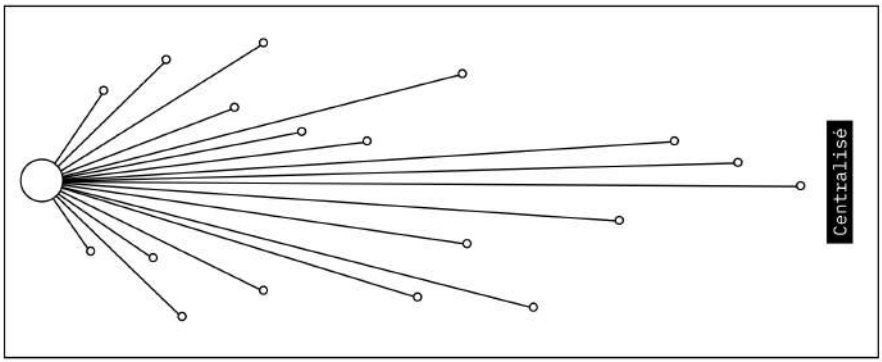
La furtivité, le besoin que notre vie privée reste privée dans un système transparent est le dénominateur commun d'une majorité d'initiatives alternatives. En faisant le choix de la furtivité, on vient se placer en opposition à la centralisation, au contrôle et à l'analyse de nos comportements. Ce désir grandissant de discrétion face à l'annexion prend de nombreuses formes, allant du minimalisme digital essayant de limiter les donneés générées, à l'obfuscation qui vise à parasiter la vision des algorythmes, en passant par le declouding qui est le retrait total du réseau, cette furtivité va de pair avec une gestion des données différente, souvent plus distribuée et respectueuse de la vie privée.

[12]A Cypherpunk's manifesto - Eric Hughes 1993 -ligne 14-17 - https://activisme.fr/cypherpunk/manifesto.html

1_La furtivité comme dénominateur commun des alternatives







Pastebin

Schéma personnel

1_La furtivité comme dénominateur commun des alternatives

La distribution d'un système permet une régulation sans forme de pouvoir central qui serait en mesure de contrôler les interactions qui s'y passent. C'est sur cette base de furtivité par la décentralisation que le bitcoin voit le jour.

En supprimant le besoin de confiance, la génération et la validation de transactions se fait de manière autonome et donc difficile à contrôler. À l'origine créé comme une alternative décentralisée et sous-jacente au système bancaire traditionnel, le bitcoin vient aujourd'hui s'ancrer dans le marché qu'il combattait, mais cette forme de furtivité a servi de preuve de concept à la blockchain, qui sert aujourd'hui de clef de voûte aux initiatives de Web 3.0[13]. Le Web 3.0, également appelé web sémantique, constitue l'ensemble des initiatives en opposition au Web 2.0 caractérisé par la consommation d'informations en continu gerée par les GAFAM.

[13]Bitcoin - https://bitcoin.org/fr/
[14]A Cypherpunk's manifesto - Eric Hughes 1993 -ligne 14-17 - https://activisme.fr/cypherpunk/manifesto.html

1_La furtivité comme dénominateur commun des alternatives

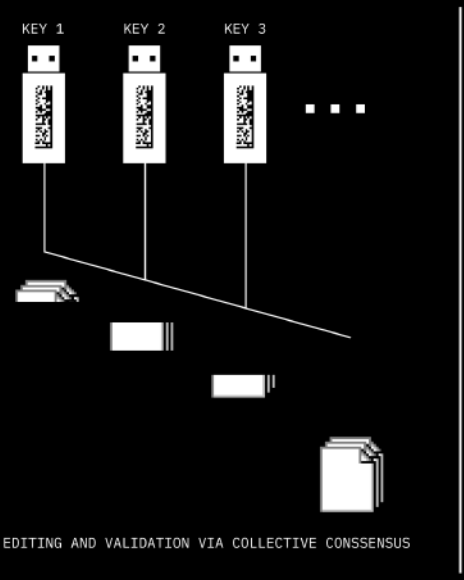
Le Web 3.0 prône l'Open Source, la distribution et la liberté d'utilisation. Le web 3.0 est actuellement le fer de lance d'une utilisation du web plus respectueuse de la vie privée des utilisateurs. Il reprend plusieurs principes de furtivité et de distribution imaginés par des acteurs de contre-culture comme la pensée cypherPunk.

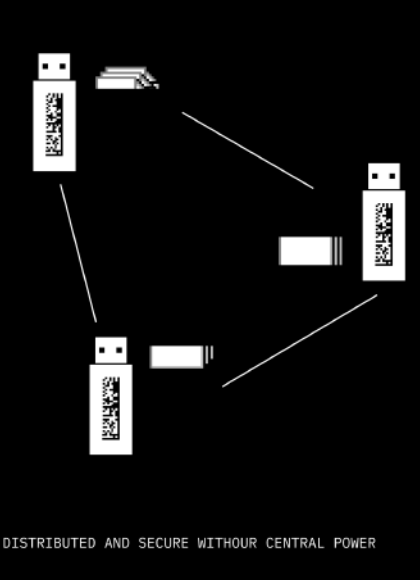
Pour expliciter de manière plus parlante les principes derrière les alternatives, et comprendre comment la notion de furtivité y est présente, j'ai réalisé une expérience visant à recréer un système de consensus sans entité de contrôle central. Ce dispositif prend la forme d'une série de clefs USB, appartenant chacun à un individu. Chaque clef est inutile seule, ce n'est qu'en les connectant toutes ensemble qu'un fichier est éditable, de manière collaborative. Une fois le consensus atteint et le fichier édité, chaque personne reprend sa clef, emportant avec elle une partie du fichier le rendant inaltérable et prouvant que son contenu est officiel. Ici le consensus est atteint de manière collaborative, la véracité est assurée par la distribution des clefs et l'impossibilité de les altérér individuellement.

[14] What is the web 3.0 ? And why it matters ? - https://medium.com/fabric-ventures/what-is-web-3-0-why-it-matters-934eb07f3d2b

1_La furtivité comme dénominateur commun des alternatives

La distribution d'un système permet une régulation sans forme de pouvoir central qui serait en mesure de contrôler les interactions qui s'y passent. C'est sur cette base de furtivité par la décentralisation que le bitcoin voit le jour.

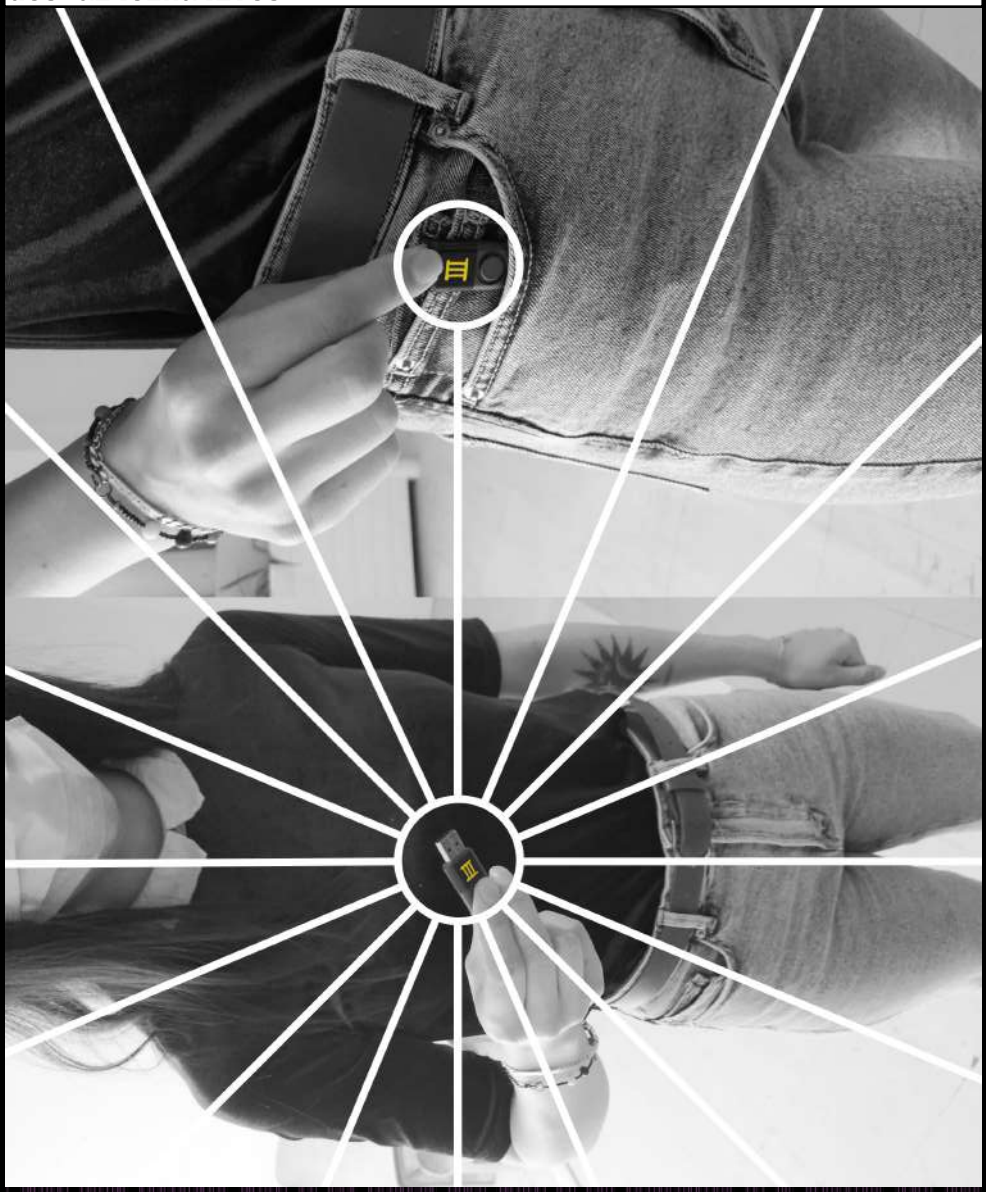




Pastebin

Schéma personnel

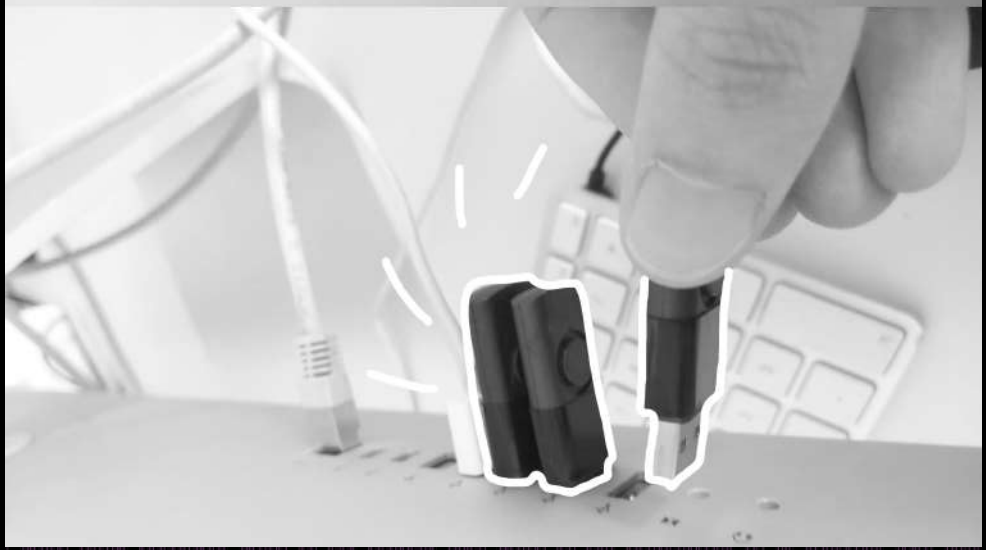
1_La furtivité comme dénominateur commun des alternatives



Pastebin

Photographie personnelle

1_La furtivité comme dénominateur commun des alternatives



Pastebin

Photographie personnelle

1_La furtivité comme dénominateur commun des alternatives

Pastebin

Photographie personnelle

2_Le spectre de la furtivité

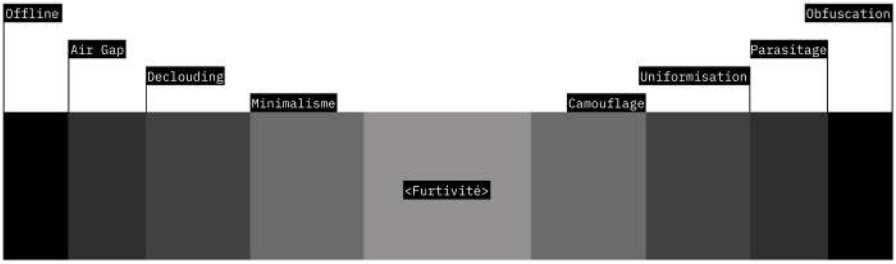
Nous avons vu la forme officielle que pouvaient prendre les initiatives alternatives avec le Web 3.0 et nous nous apprêtons à plonger plus profondément dans les couches de chiffrement, pour aller retrouver les initiatives d'indépendants, utilisant le web d'une manière bien plus cryptique. Souvent associée à l'illégalité, la furtivité crée une sorte de fascination, au même titre que l'anonymat. Il suffit de voir l'engouement généré autour de l'inventeur supposé du Bitcoin pour se rendre compte que le fait de ne pas savoir est un terreau fertile à tous les plus grands fantasmes.

Derrière cette idée de furtivité pour camoufler un comportement illégal, résonne cependant une part de vérité, puisque les premières adoption de technologies anonymisantes sont souvent effectuées par des personnes partcipant à des activités nécéssitant un haut degré de discrétion. Cependant il est important de se rendre compte qu'à l'heure actuelle, la discrétion n'est pas systématiquement liée à l'illégalité, et sert majoritairement des causes considérées comme justes, comme la protection de la vie privée.

[14] What is the web 3.0 ? And why it matters ? - https://medium.com/fabric-ventures/what-is-web-3-0-why-it-matters-934eb07f3d2b

2_Le spectre de la furtivité

Le réseau TOR, pour "The Onion Router"[15], est le fruit d'un travail de recherche Open source visant à proposer un navigateur Web sécurisé, chiffré et anonymisant. Dans ce projet, la furtivité est atteinte par l'uniformisation. En effet si tout le monde se ressemble à l'identique, il est très difficile de traquer qui que ce soit. Si je suis partout, je suis nulle part. Afin de mieux cerner quelles formes prend la furtivité et voir quelles répercussions elle engendre sur l'usage, qu'il soit numérique ou physique, nous pouvons dresser un spectre de la furtivité.



[15]The TOR project - https://www.torproject.org/

2_Le spectre de la furtivité

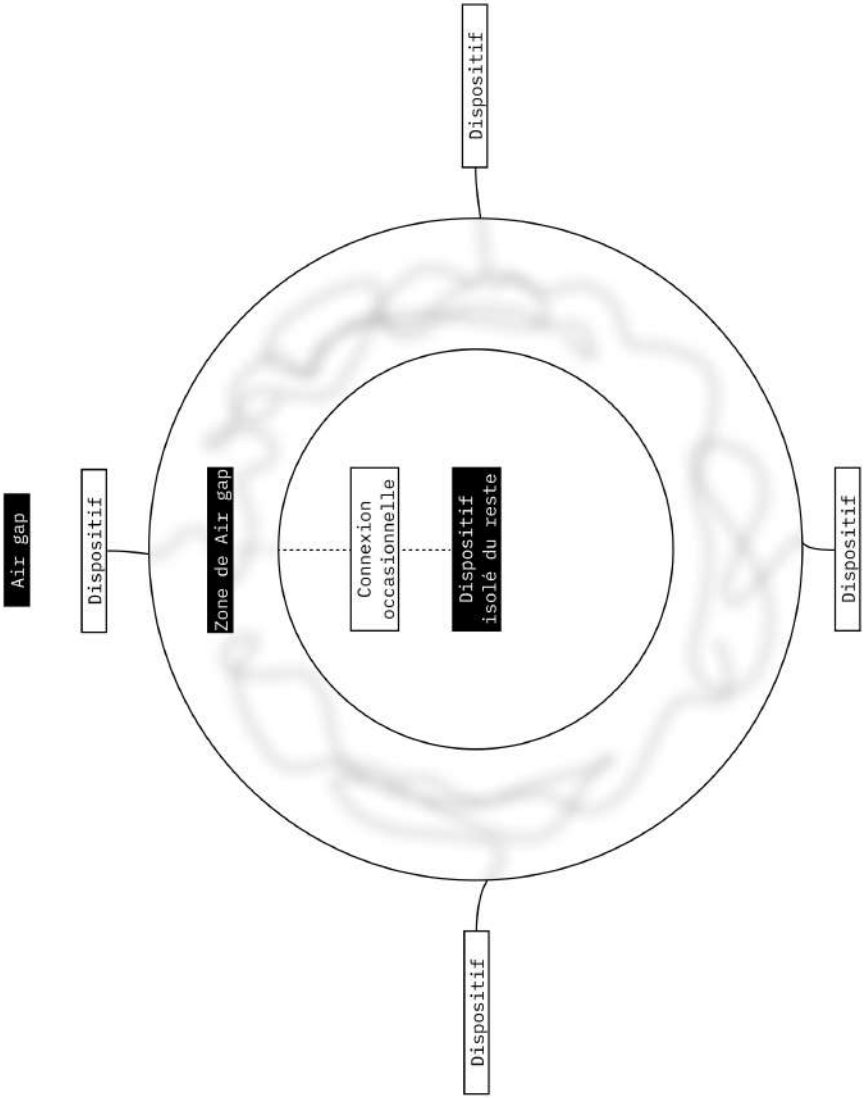
Étant un procédé malléable, la furtivité peut par exemple prendre la forme de l'hérmétisme, également appelée Air Gap. Ce mode de furtivité assez extrême dans sa démarche se caractérise par un "espace d'air" entre plusieurs dispositifs qui les isolent les uns des autres. Cette méthode vise à constituer une alternative qui n'a pas, ou très peu, de porosité avec d'autres systèmes et donc internet. Si l'ensemble des alternatives peut être qualifié d'Alternet, cette forme de communication off grid ne souhaitant pas d'hybridation peut alors être appelée l'Externet. Le créateur de contenu N-O-D-E présente une itération de ce principe au travers d'un système de communication Off-Grid ne fonctionnant qu'en se reposant sur ses propres dispositifs mobiles[16]. Dans le cas de cette réalisation, la faible porosité avec d'autres systèmes permet un anonymat et une autonomie quasi totale, ne reposant sur aucunes infrastructures à distance. Ce projet frôle même le Offline qui est la déconnection totale avec internet, en tentant de créer son propre réseau nodal distribué.

Cette pratique implique de lourdes répercussions sur l'usage et sur notre manière de communiquer en elle-même car possédant une rapidité et un volume de données drastiquement différents à ce dont nous sommes habitués.

Pastebin

[16]HELP BUILD AN OFF GRID COMMUNICATIONS - N-O-D-E - https://n-o-d-e.net/meshdevice.html

2_Le spectre de la furtivité



Pastebin

Schéma personnel

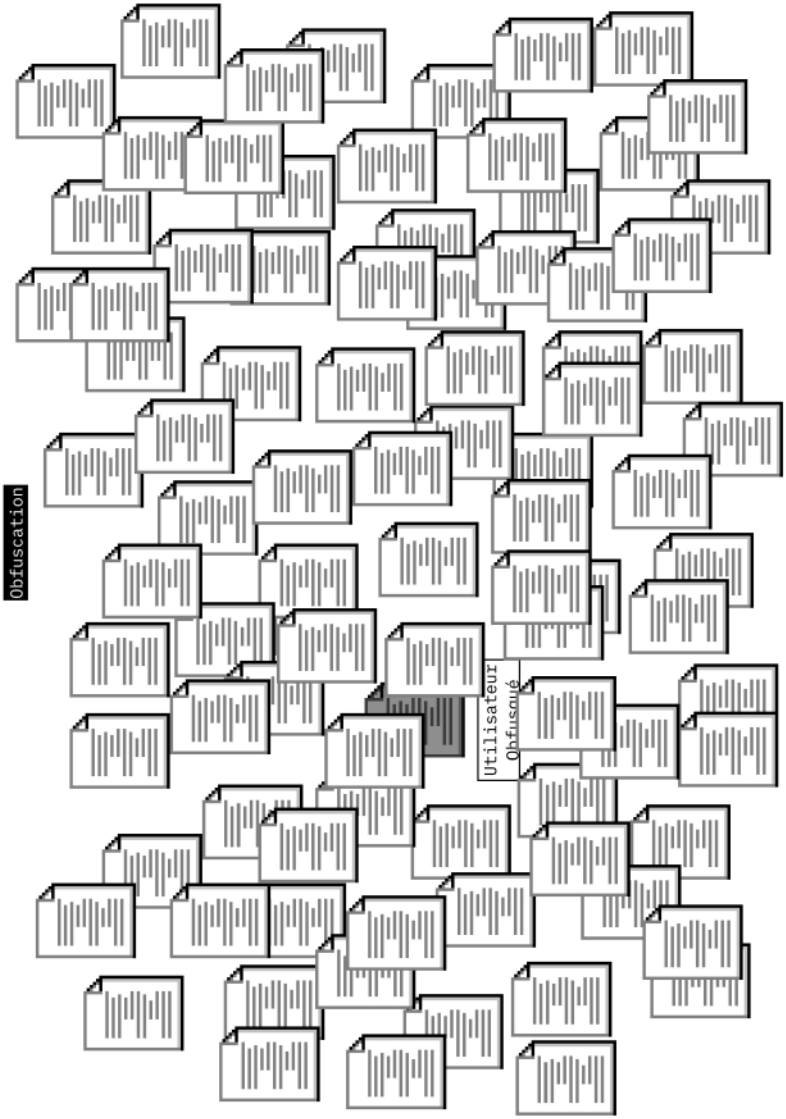
2_Le spectre de la furtivité

À l'opposé, sur ce que nous allons désormais appeler le spectre de la furtivité, se citue l'obfuscation. L'obfuscation est une autre manière d'aborder la furtivité, qui pourrait être résumée de la manière suivante "si je déploie trop de données superflues, je suis cachée parmi elles." Le principe est donc de prendre le contrepied du minimalisme digital ou du air gap, qui tous deux consistent à générer le moins de données analysables possibles. Dans cette forme de furtivité, une logique de parasitage vient s'ajouter.

Si l'on prend l'exemple de TrackMeNot[17], une application permettant de brouiller le fichage de nos recherches internet en générant d'autres recherches aléatoires, une nouvelle étape de la furtivité est atteinte. Non seulement nous sommes cachés parmi la masse de données insubstantielles générées, mais en plus nous saturons les algorythmes en leur injectant des données erronées, enrayant par la même occasion leur fonctionnement.

[17] Obfuscation, a user's guide for privacy and protest - Finn Brunton et Helen Nissenbaum

2_Le spectre de la furtivité



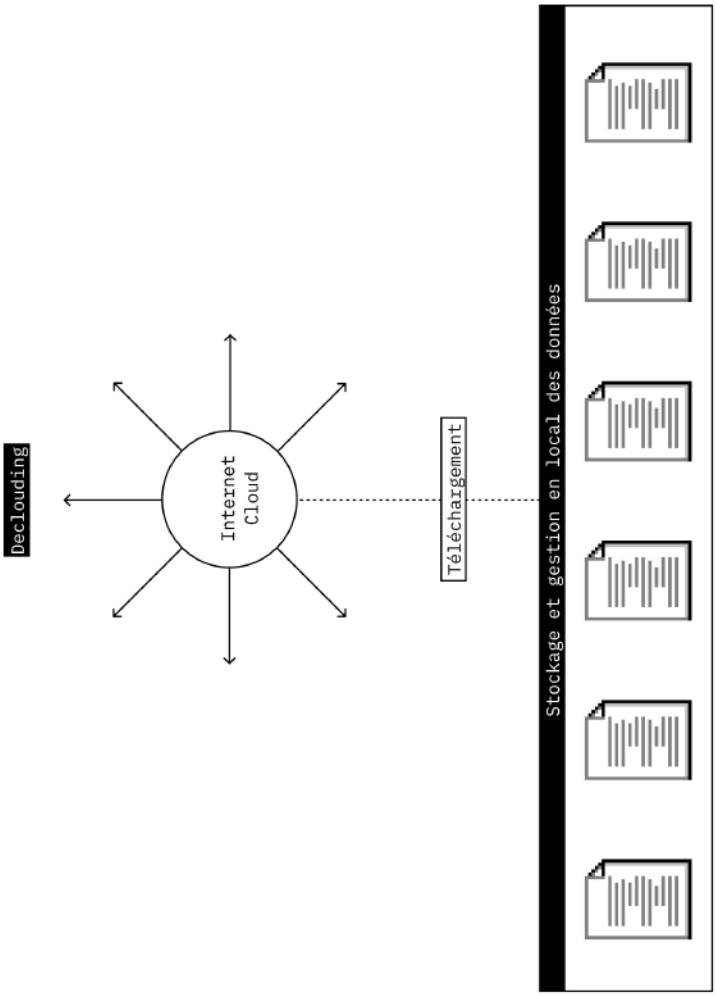
Pastebin

[17]Obfuscation, a user's guide for privacy and protest - Finn Brunton et Helen Nissenbaum - principe mis en schéma

2_Le spectre de la furtivité

La logique de décloud ing est également intéressante dans sa manière de traiter la discrétion et la furtivité. Proche du air gap décrit plus haut, cette démarche s'inscrit en opposition avec la tendance actuelle qui vise l'ubiquité numérique. Les services actuels, toujours plus puissants et exigeants en ressources, forcent par leurs fonctionnement une dépossession des données des utilisateurs au profit d'utilisation de cloud, et d'infrastructures de calculs à distance. Ce modèle vise donc une omniprésence de services distants dans nos vies pour plus de performance et de fluidité. Venir lutter contre ce phénomène revient donc à modifier son utilisation et rejetter le stockage à distance pour redevenir maître de nos données.

En décloudant, on retourne à des logiques de calcul et de stockage sur nos propres machines, ayant donc un meilleur contrôle sur elles. Ce modèle en opposition totale avec ce vers quoi tendent les GAFAM, nécessite de réapprendre un certain nombre de pratiques. Notre utilisation peut se voir restreinte, ou à minima repensée par la limitation technique de nos appareils ne disposant plus d'une assistance à distance.



Pastebin

Schéma personnel

2_Le spectre de la furtivité

Pour souligner l'impact du déclouding sur une utilisation classique, j'ai essayé de l'intégrer dans la logique de transaction bancaire au travers d'une expérimentation. Le but de cette expérimentation est de voir s'il est possible de relocaliser les échanges bancaires, tout en rendant le principe réalisable n'importe où. Pour ce faire, j'ai voulu faire croiser le Bitcoin, une cryptomonnaie universelle et décentralisée, avec un support d'échange physique et low-tech : les cassettes audio.

Dans les années 80, le "commerce local" de cassettes piratées ou dupliquées impliquait des interactions furtives et non régulées. Pour fusionner ces deux univers, j'ai donc édité une transaction de Bitcoin que j'ai transcodé et chiffré en son à l'aide d'un logiciel de conversion en 16BIT pour l'inscrire sur la bande magnétique de la cassette audio. De ce fait, on obtient un nouvel objet de transaction, décloudé, n'utilisant une connection qu'au moment initial de son édition et au moment final de sa validation.

2_Le spectre de la furtivité

Procédé de création de la crypto-cassette :

Principe

Voir si il est possible de relocaliser les échanges monétaire d'une cryptomonnaie qui est mondiale et universelle, en esseyant de croiser le commerce de cassette audio pirates avec des transactions de Bitcoin.

Procédé

Convertir une transaction Bitcoin en son puis la chiffrer avant de l'enregistrer sur la bande magnétique d'une cassette audio. Utiliser audacity et un ordinateur 16bit de récupération ou un raspberry Pi 3B.

Mise en application

L'inscription sur la cassette ainsi que les transactions se font donc sans aucune connection, seulement via le passe passe des cassettes de manières anonymes et intraçables. Seule la validation est officielle.

2_Le spectre de la furtivité

Pastebin

Photographie personnelle

2_Le spectre de la furtivité

2_Le spectre de la furtivité

Cette expérimentation témoigne de la liaison forte entre annexion de la vie privée numérique et impact sur le terrain.

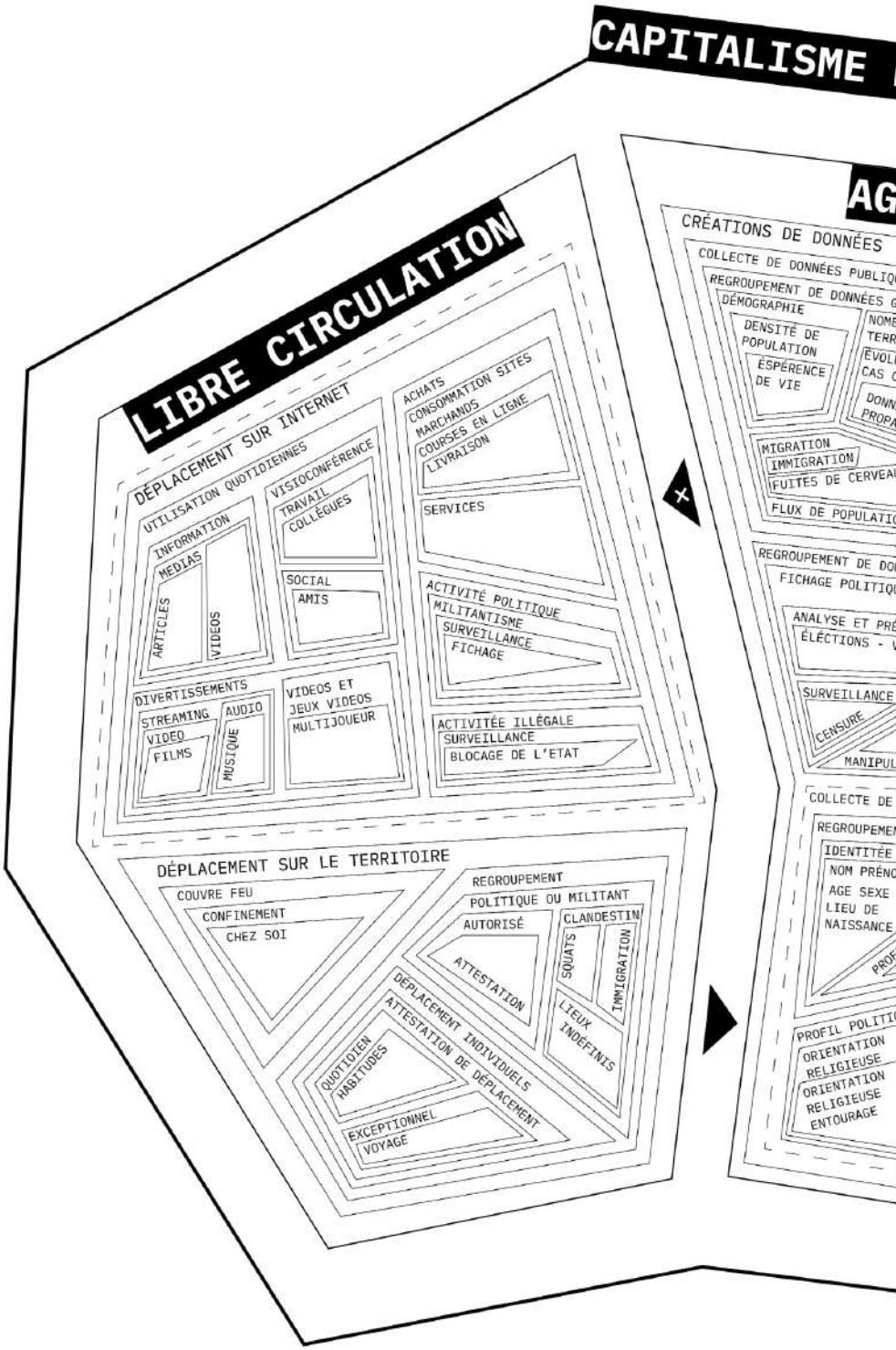
Le monde numérique et le monde réel ne sont pas deux sphères indépendantes et hermétiques, elles sont interconnectés. Cette notion de physicalité du net, de voir internet comme un territoire, implique son évolution avec d'autres territoires, eux physiques. Le travail de cartographie de Louise Druhle "*Critical Atlas of the Internet*"[18] part du principe suivant : si internet est une forme de territoire, alors il faut le cartographier à l'aide d'outils hypothétiques. Le but ses recherches est de questionner les impacts physiques, économiques et sociaux d'internet et de leur donner une forme reprennnant celle de la cartographie de territoire physique.

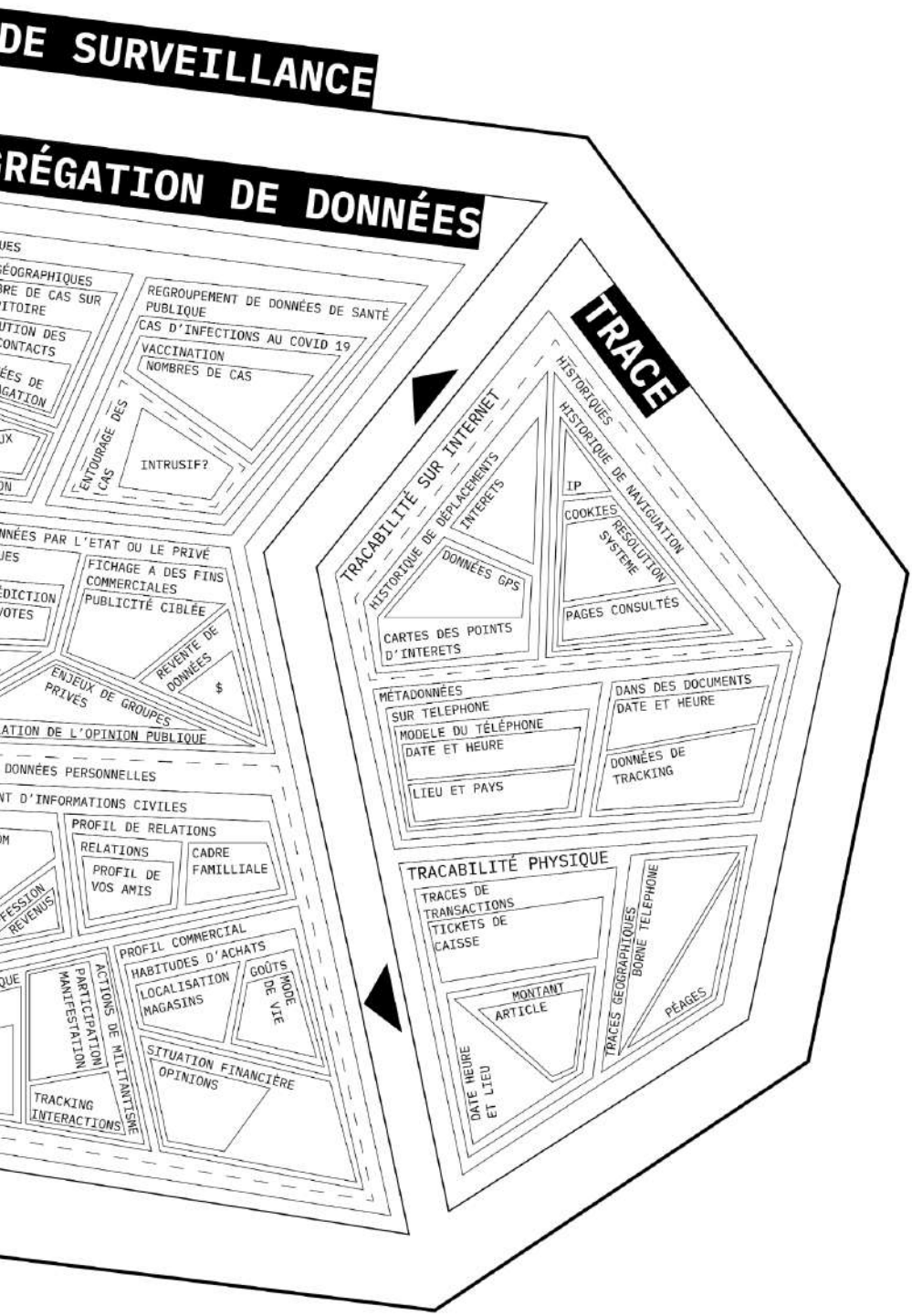
Le résultat de sa démarche est un atlas matérialisant les interactions entre actions numériques et territoire physique.

[18] Critical Atlas Of The Internet, Spatial analysis as a tool for socio-political purposes - Louise Druhle - https://louisedrulhe.fr/internet-atlas/

2_Le spectre de la furtivité

Pour m'ancrer dans la continuité de la démarche, j'ai voulu représenter en quoi phénomènes dans le monde tangible, tels que l'actuelle pandémie du Covid-19 a un impact sur l'utilisation de nos données, et vice-versa comment l'agrégation de nos données numériques peut avoir un impact sur nos déplacements physiques en temps de crise. Pour ce faire, j'ai réalisé les plans d'une sorte de *forteresse de données*, à partir de données du covid-19 dont les interactions sont parfois obscures pour le grand public.


CAPITALISME
AG
LIBRE CIRCULATION
DÉPLACEMENT SUR INTERNET
UTILISATION QUOTIDIENNES
INFORMATION
MEDIAS
ARTICLES
VIDEOS
VISIOCONFÉRENCE
TRAVAIL
COLLÈGUES
SOCIAL
AMIS
DIVERTISSEMENTS
STREAMING
VIDEO
FILMS
AUDIO
MUSIQUE
VIDEOS ET
JEUX VIDEOS
MULTIJOUEUR
ACHATS
CONSOMMATION SITES
MARCHANDS
COURSES EN LIGNE
LIVRAISON
SERVICES
ACTIVITÉ POLITIQUE
MILITANTISME
SURVEILLANCE
FICHAGE
ACTIVITÉE ILLÉGALE
SURVEILLANCE
BLOCAGE DE L'ETAT
DÉPLACEMENT SUR LE TERRITOIRE
COUVRE FEU
CONFINEMENT
CHEZ SOI
REGROUPEMENT
POLITIQUE OU MILITANT
AUTORISÉ
ATTESTATION
CLANDESTIN
SQUATS
IMMIGRATION
LIEUX INDÉFINIS
DÉPLACEMENT INDIVIDUELS
ATTESTATION DE DÉPLACEMENT
QUOTIDIEN
HABITUDES
EXCEPTIONNEL
VOYAGE
CRÉATIONS DE DONNÉES
COLLECTE DE DONNÉES PUBLIQ
REGROUPEMENT DE DONNÉES
DÉMOGRAPHIE
DENSITÉ DE
POPULATION
ESPÉRENCE
DE VIE
MIGRATION
IMMIGRATION
FUITES DE CERVEA
FLUX DE POPULATI
REGROUPEMENT DE DO
FICHAGE POLITIQ
ANALYSE ET PR
ÉLECTIONS -
SURVEILLANCE
CENSURE
MANIPUL
COLLECTE DE
REGROUPEMEN
IDENTITÉE
NOM PRÉNO
AGE SEXE
LIEU DE
NAISSANCE
PROF
PROFIL POLITI
ORIENTATION
RELIGIEUSE
ORIENTATION
RELIGIEUSE
ENTOURAGE


DE SURVEILLANCE
RÉGATION DE DONNÉES
TRACE
TRACABILITÉ SUR INTERNET
HISTORIQUES
HISTORIQUE DE DÉPLACEMENTS
INTERETS
HISTORIQUE DE NAVIGUATION
IP
COOKIES
RÉSOLUTION
SYSTEME
DONNÉES GPS
PAGES CONSULTÉS
CARTES DES POINTS D'INTERETS
MÉTADONNÉES
SUR TELEPHONE
MODELE DU TÉLÉPHONE
DATE ET HEURE
LIEU ET PAYS
DANS DES DOCUMENTS
DATE ET HEURE
DONNÉES DE TRACKING
TRACABILITÉ PHYSIQUE
TRACES DE TRANSACTIONS
TICKETS DE CAISSE
MONTANT
ARTICLE
DATE HEURE ET LIEU
TRACES GEOGRAPHIQUES
BORNE TELEPHONE
PÉAGES
UES
ÉOGRAPHIQUES
RE DE CAS SUR
ITOIRE
UTION DES
CONTACTS
ÉES DE
GATION
JX
ON
REGROUPEMENT DE DONNÉES DE SANTÉ PUBLIQUE
CAS D'INFECTIONS AU COVID 19
VACCINATION
NOMBRES DE CAS
ENTOURAGE DES CAS
INTRUSIF?
NNÉES PAR L'ETAT OU LE PRIVÉ
UES
ÉDICTION
VOTES
FICHAGE A DES FINS COMMERCIALES
PUBLICITÉ CIBLÉE
REVENTE DE DONNÉES
$
ENJEUX DE GROUPES PRIVÉS
ATION DE L'OPINION PUBLIQUE
DONNÉES PERSONNELLES
NT D'INFORMATIONS CIVILES
PROFIL DE RELATIONS
RELATIONS
PROFIL DE VOS AMIS
CADRE FAMILLIALE
OM
FESSION
REVENUS
QUE
PROFIL COMMERCIAL
HABITUDES D'ACHATS
LOCALISATION MAGASINS
GOÛTS
MODE DE VIE
ACTIONS DE MILITANTISME
PARTICIPATION MANIFESTATION
SITUATION FINANCIÈRE
OPINIONS
TRACKING INTERACTIONS

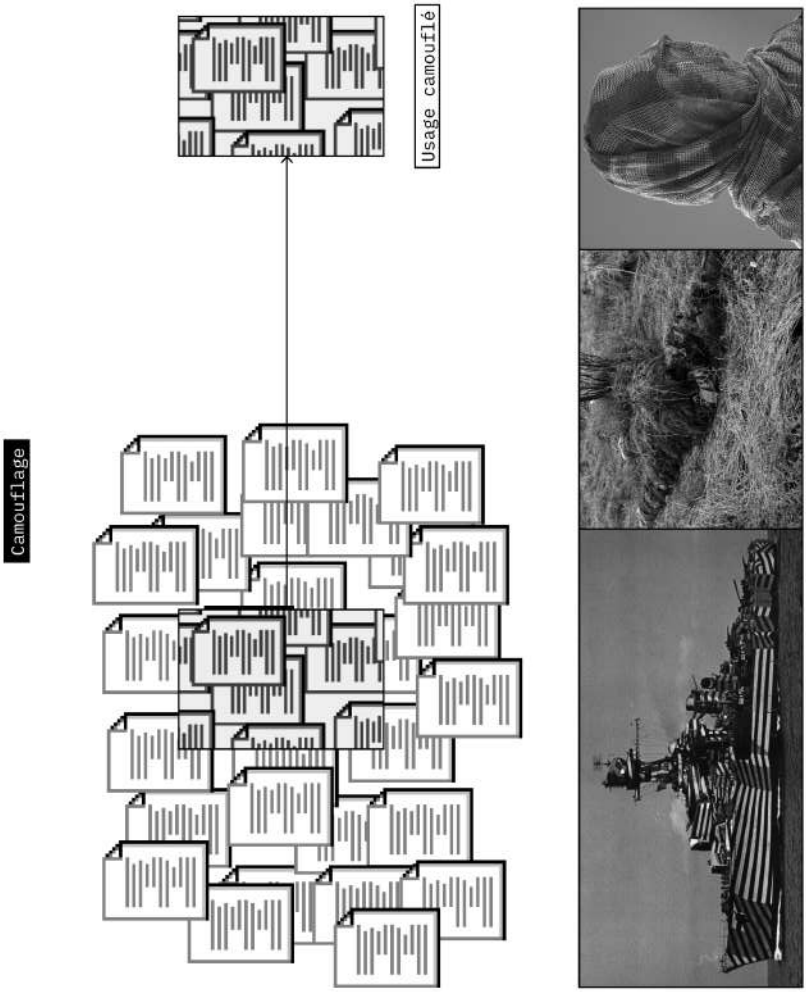
2_Le spectre de la furtivité

Le meilleur exemple de l'annexion de la vie privée qui se matérialise dans le monde physique au travers d'intéractions numériques est la surveillance des lieux publics. Les caméras de surveillance posent le problème de la vie privée physique, qui est elle aussi espionnée et croisée avec la récolte de notre comportement sur le net. Cette double analyse, physique et numérique, implique une modification de notre comportement en temps que personne si l'on souhaite s'en émanciper.

L'artiste Ceren Paydas mobilise ce concept de protection physique contre des problèmes d'ordres numériques au travers de sa QT Scarf, un écharpe modifiée émettant une lumière infrarouge rendant son visage non reconnaissable par des caméras de surveillance. Dans son initiative, l'artiste fait preuve de furtivité au travers du camouflage, qui fait écho aux techniques de discrétion les plus anciennes. On voit donc que la forme que prend la furtivité est changeante, et que celle-ci implique des adaptations et des transformations en termes de gestion, d'utilisations, de comportement, que ce soit du côté de celui qui créé le service, ou du côté de celui qui l'utilise. Ces deux rôles sont parfois confondus avec une réapropriation ou une personalisation poussée de l'expérience par les utilisateurs. Ainsi nous allons voir les répercutions d'usages qu'engendre Alternet.

[19] QT scarf - Ceren Paydas - https://www.cerenp.com/q-t-scarf/

2_Le spectre de la furtivité



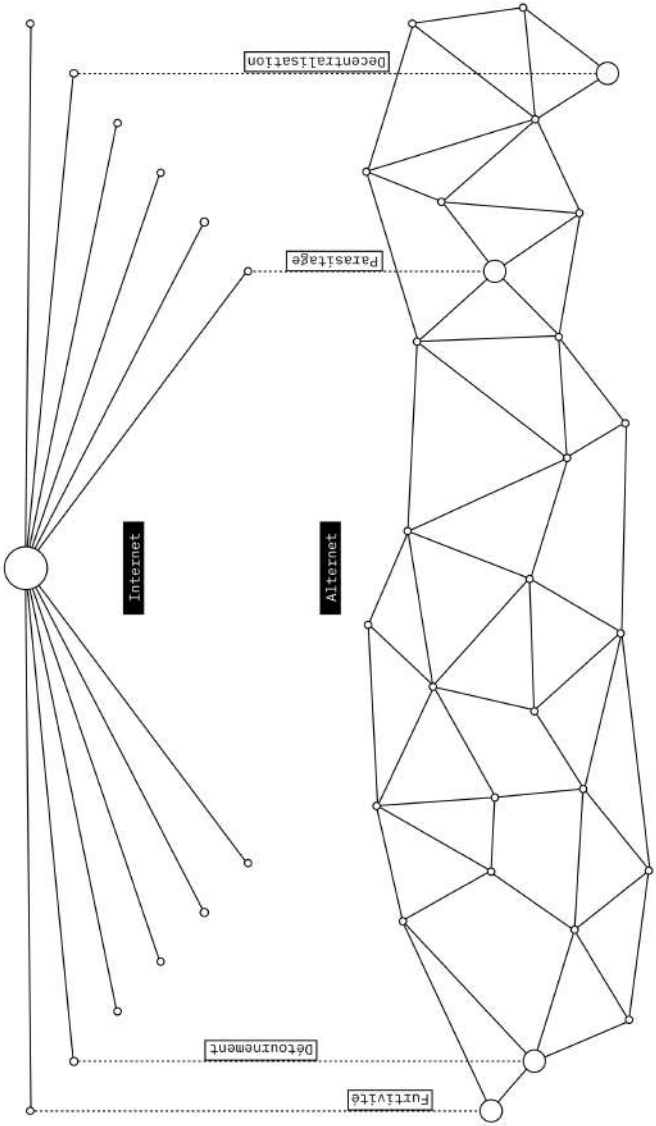
Pastebin

Schéma personnel

2_Le spectre de la furtivité

Au regard de ce que nous avos compris sur l'ensemble des initiatives alternatives, et sur l'Alternet, nous pouvons faire évoluer notre schéma de base qui nous sert a conceptualiser l'alternet.

2_Le spectre de la furtivité



Pastebin

Schéma personnel

une densité et temporalité différente

UneDensitéEtTemporalitéDifférenteUneDensitéEtTempo
ralitéDifférenteUneDensitéEtTemporalitéDifférenteU
neDensitéEtTemporalitéDifférenteUneDensitéEtTempor
alitéDifférenteUneDensitéEtTemporalitéDifférenteUn
eDensitéEtTem

0x	30	0x	20	0x	09	0x	31	0x	20
0x	09	0x	31	0x	20	0x	09	0x	32
0x	20	0x	09	0x	33	0x	20	0x	09
0x	35	0x	20	0x	09	0x	38	0x	20
0x	09	0x	31	0x	33	0x	20	0x	09
0x	32	0x	31	0x	20	0x	09	0x	33
0x	34	0x	20	0x	09	0x	35	0x	35
0x	20	0x	09	0x	38	0x	39	0x	20
0x	09	0x	31	0x	34	0x	34	0x	20
0x	09	0x	32	0x	33	0x	33	0x	20
0x	09	0x	33	0x	37	0x	37	0x	20
0x	09	0x	36	0x	31	0x	30	0x	20
0x	09	0x	39	0x	38	0x	37	0x	20

解决方案列在所有页面上

sitéEtTempora
litéDifférente
DensitéEtTemp
ensitéEtTempo
téDifférenteU
nsitéEtTempor
éDifférenteUn
sitéEtTempora
DifférenteUne
itéEtTemporal
ifférenteUneD
téEtTemporali
fférenteUneDensitéEtTemporalitéDifférenteUneDensit
éEtTemporalitéDifférenteUneDensitéEtTemporalitéDif
férenteUneDensitéEtTemporalitéDifférenteUneDensité
EtTemporalitéDifférenteUneDensitéEtTemporalitéDiff
érenteUneDensitéEtTemporalitéDifférenteUneDensitéE
tTemporalitéDifférenteUneDensitéEtTemporalitéDiffé
renteUneDensitéEtTemporalitéDifférenteUneDensitéEt
TemporalitéDifférenteUneDensitéEtTemporalitéDiffér
enteUneDensitéEtTemporalitéDifférenteUneDensitéEtT
emporalitéDifférenteUneDensitéEtTemporalitéDiffére
nteUneDensitéEtTemporalitéDifférenteUneDensitéEtTe
mporalitéDifférenteUneDensitéEtTemporalitéDifféren
teUneDensitéEtTemporalitéDifférenteUneDensitéEtTe
men

Il est important de comprendre qu'éviter l'utilisation de services grand public et performants n'est pas systématiquement synonyme de retour en arrière. Il est indéniable que dans certaines applications, les moyens et l'expérience mise en œuvre par des services ayant des budgets titanesques seront plus performants, mais la performance, la rapidité et l'instantanéité n'est pas forcément le but d'Alternet. Pour la plupart, ces initiatives impliquent une gestion différente avec des densités de données moins importantes et plus réfléchies.

Là où les services appartenant au web 2.0 accélèrent la consommation de contenus et d'informations, bien souvent, Alternet vient redonner le choix de la temporalité à ses utilisateurs. Par ce choix, de nouvelles problématiques se posent. Comment communiquer ou créer du contenu qui vise une réception en différé contrairement à une consommation instantanée comme actuellement par exemple. On peut alors dire qu'une des répercussions de la furtivité est la patience.

1_Un espace temps altéré pour la furtivité

Au travers du cas des *Dead drops*[20], un réseau de partage d'informations Offline sur des clefs USB emmurées, on percoit des problématiques d'usage qui concerne la durée d'acheminement, rappelant l'exemple du courrier envoyé par voie postale. Un tel principe de partage très local et à la temporalité lente rappelle également la bouteille à la mer, et implique de se déplacer physiquement pour accéder au lieu de partage. Ces approches sont un contrepied total à l'accessibilité constante et mobile vendues par les services actuels. Ici la temporalité est drastiquement différente car elle prend le parti du Offline, freinant considérablement la vitesse des échanges, mais rendant sa régulation impossible.

Les volumes de données en circulation sont également altérés, revus pour s'adapter à la furtivité. Basculer d'une utilisation centralisée et instantanée à une utilisation décentralisée et Peer To Peer implique de repenser la nature de nos échanges. Dans le peer to peer, qui revient à se connecter directement à un autre utilisateur sans passer par une infrastructure à distance, la connexion des deux destinataires est souvent nécéssaire et induit une réciprocité plus marquée qu'avec les centaines de notifications que nous recevons chaque jour.

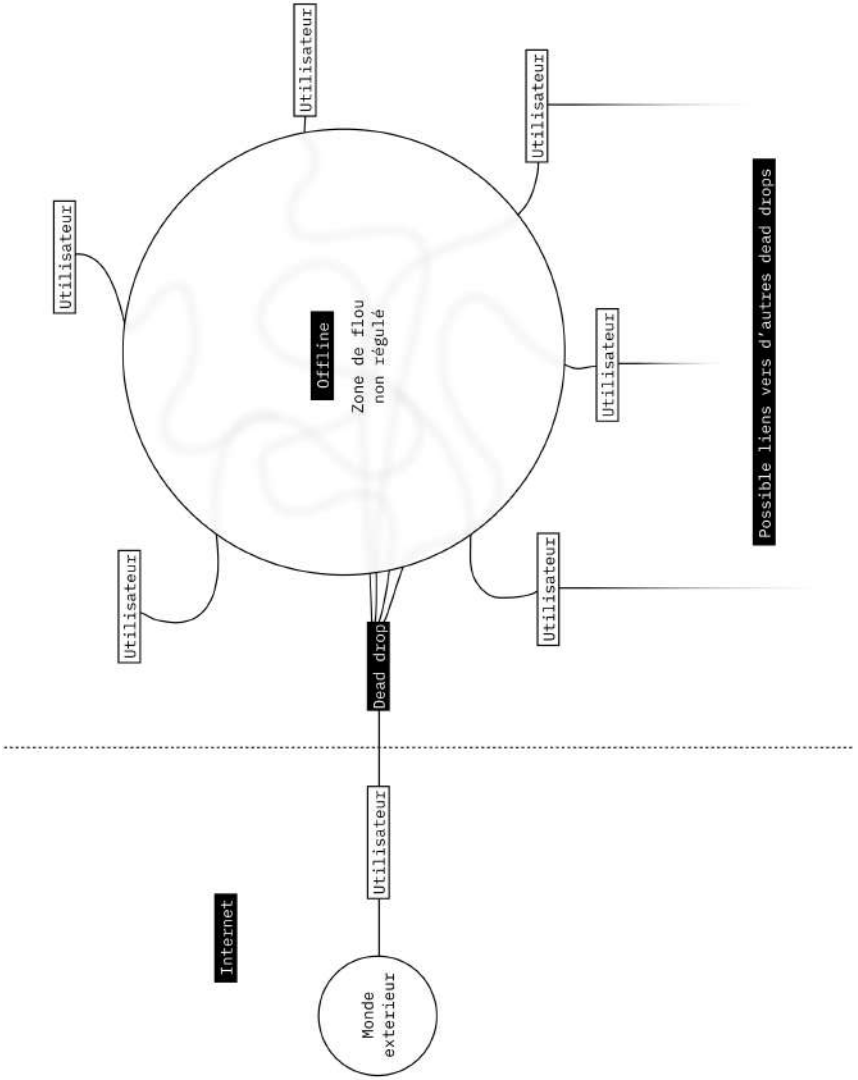
[20] Dead drop - Aram Bartholli - https://deaddrops.com/db-map-2/

Citton critique ce principe de surconsommation de données en parlant de *double fantomisation*[21]. Le monde, en état d'hyper disponibilité, est réduit à l'état de fantôme au même titre que le spectateur. On vient confondre la présence, qui est une forme de contact au monde réel et l'instantanéité qui est la simple notion de rapidité avec laquelle les images du monde nous sont montrées. Ainsi, les approches décentralisées, par leur contrainte due à leur lenteur, induisent un ralentissement et un besoin de réfléchir sur la nature des données à échanger.

Contraints par des appareils plus lent, ces pratiques peuvent être perçues comme une forme d'assainissement par la latence et la limitation nécéssaire au fonctionnement sein du système. De plus, en tant que designer venant du milieu du design d'objet industriel, la question de la mise en place et du déploiement de ces alternatives sur le terrain entre en jeu. La mise en place n'est pas aussi simple car l'idée de créer une infrastructure décentralisée, ou Peer to Peer ne peut pas être intégrée en fin de course mais doit être implémentée à la racine du developpement d'un projet. Dans ce cas, penser des logiques de déploiement pour manifester ces principes numériques dans le monde réel permet de physicaliser la démarche des alternatives.

[21] Yves Citton. « Médiarchie », pp. 939-340, citant Günther Anders, L'Obsolescence de l'homme p. 151, 155-156.

1_Un espace temps altéré pour la furtivité



Pastebin

Schéma personnel

2_Le déploiement physique de principes numériques

Dans le manifeste cypherpunk, une phrase très connue résonne : "les cypherpunks écrivent du code". En écrivant cette phrase, Eric Huhges ancre la pensée cypherpunk dans le monde du code et de la création de logiciels. Mais les changements d'utilisation qu'impliquent les principes qui régissent la pensée cypherpunk nous poussent à revoir certaines formes de dispositifs. Adapter la démarche numérique du cypherpunk au monde tangible.

C'est pourquoi, penser de nouvelles infrastructures est important. Il s'agit de manifester Alternet dans la réalité au travers de nouveaux dispositifs qui seront support de de nouveaux usages. Harvest, un dispositif de minage de cryptomonnaie off-grid, produisant sa propre éléctricité grâce à des éoliennes est une forme de dispositif alternatif avec un but critique. Dans ce dispositif de critical engineering, on percoit la possibilité de créer nos propres dispositifs de création de valeur, bien que cet exemple soit plus manifeste que fonctionnel.

2_Le déploiement physique de principes numériques

Pour continuer sur cette logique de déploiement dans le monde réel, mais cette fois-ci de manière rapide et éphémère, les outils de Backlash cherchent à mettre en place un réseau de communication d'urgence dans des manifestations tendues. Au travers de ces deux exemples, on constate une similarité, qui est la réapropriation et le détournement de matériel, qui plus globalement, est commun à la plupart des initiatives indépendantes.

Par la nature "non officielle" et furtive d'Alternet, il est normal que la mise en place de tels dispositifs se fasse par la réapropriation de matériel déjà existant. Avec le détournement, on vient rompre, détacher, isoler un élément de technologie pour en faire quelque chose d'autre. Ceci revient à le soustraire à sa fonction centralisée de base. De ce fait, en coupant les ponts avec leurs créateurs, on peut se servir des technologies de manière plus libre, anonyme et donc plus furtive.

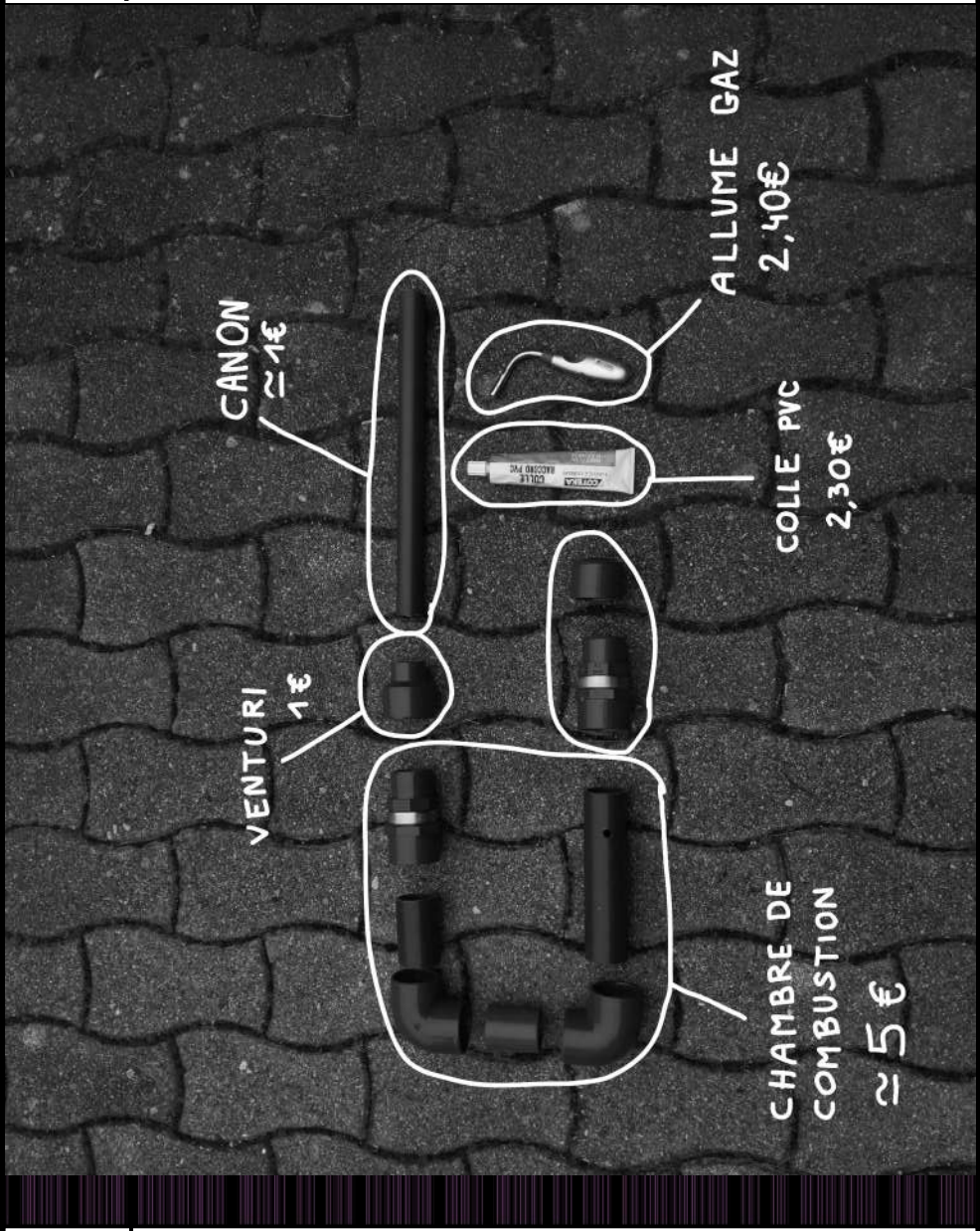
[23]Backlash - Pedro G. C. Oliviera & Xuedi Chen - p 25-28 https://www.disobedientelectronics.com/resources/Hertz-Disobedient-Electronics-Protest-201801081332c.pdf

2_Le déploiement physique de principes numériques

Pour investir cette logique de déploiement, j'ai tenté de créer un dispositif de communication, avec un accent particulier sur son déploiement au sens littéral. L'idée est de questionner la longévité de tels dispositifs à moyen ou long terme en contraste avec les initiatives de Backlash, souvent trop éphemeres, en essayant de voir comment ces dispositifs peuvent s'intégrer en hybridation ou en parasitage avec d'autres services déjà existants. En constituant des objets avec une durée de vie plus longue, on peut essayer de créer des usages en pensant la durée de vie du dispositif, en prenant en compte sa recharge, son entretien, son devenir après utilisation, etc.

Ici j'ai imaginé et réalisé un prototype de lanceur logistique, ayant pour but la mise en place rapide d'un dispositif de parasitage radio. Ce prototype vient poser la question de l'implication physique de l'utilisateur, car il doit aller déployer le systeme et donc s'engager corporellement dans la démarche. Le prototype prend la forme d'un lance projectile très facile à faire et connu sur internet, mais je viens ici le convertir en outil de lutte, voire de nuisance. Étant fait pour etre démonté et transportable facilement dans un sac, tout en ne dépassant pas la dixaine d'euros pour sa réalisation, cet outil logistique peut être utilisé pour déployer différents types d'objets supports de communication. Le projectile et le canon étant les deux seules parties à faire varier pour déployer tout type de systèmes.

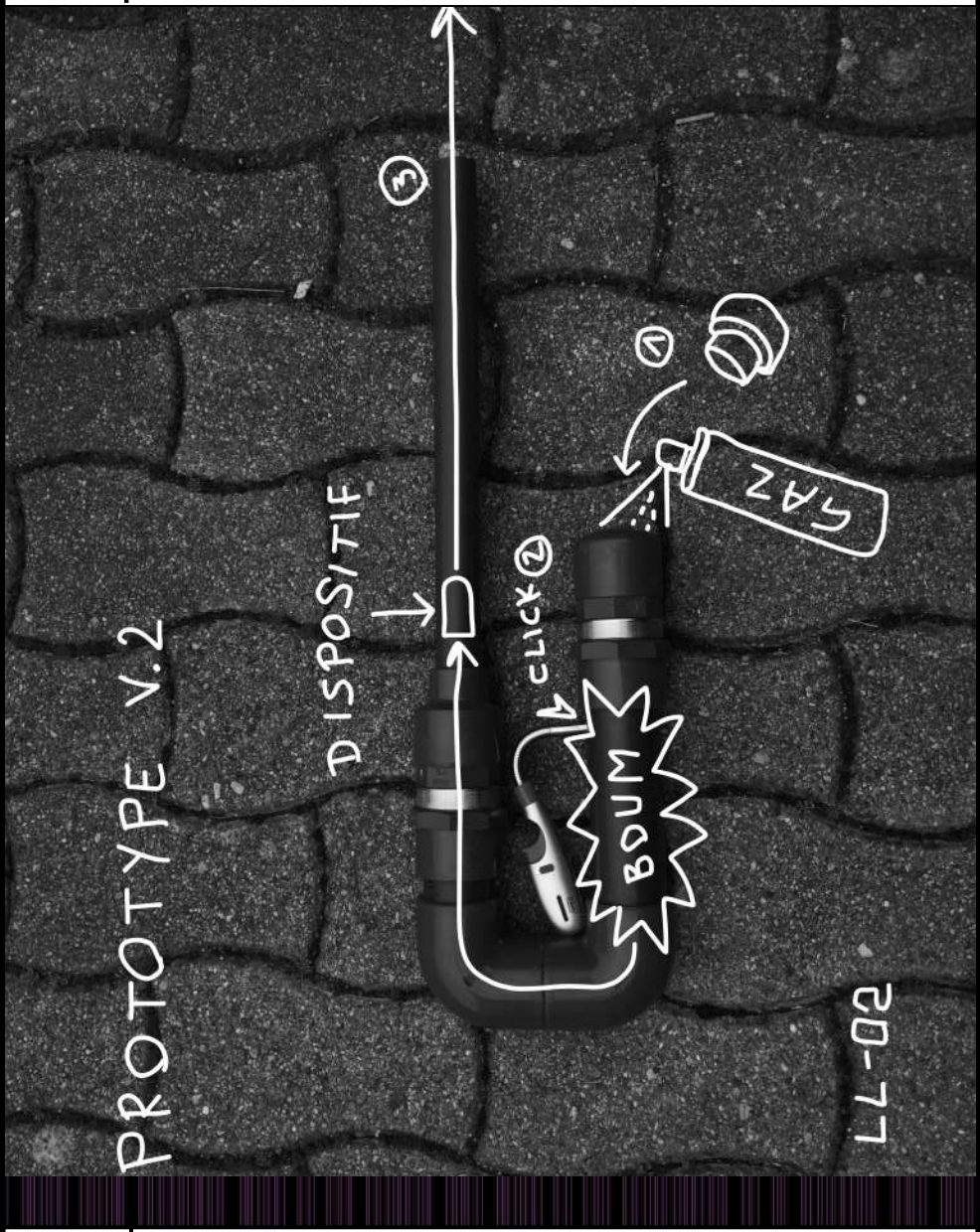
2_Le déploiement physique de principes numériques



Pastebin

Photographie personnelle

2_Le déploiement physique de principes numériques



Pastebin

Photographie personnelle

2_Le déploiement physique de principes numériques

Pastebin

Photographie personnelle

Pastebin

Photographie personnelle

2_Le déploiement physique de principes numériques

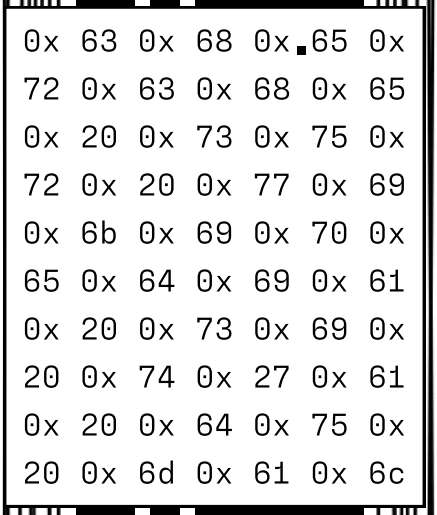
À travers cette pratique ressort la nécéssité de ne plus fermer les principes du cypherpunk au monde du numérique, mais de venir le manifester de manière tangible dans la réalité. Cette notion de manifester la furtivité peut sembler paradoxale mais c'est avec la création de dispositifs de furtivité que la mise en place de ces pratiques peuvent voir le jour.

Avec une logique de parasitage ou de remplacement de communication comme illustré dans la dernière expérimentation, on vient réinvestir les sytèmes numériques en place par un déploiement et une action physique. Ces objets manifestés sont donc les supports de la furtivité d'Alternet.

3_Des répercussions politico-techniques et sociales ?

La mise en place de ces initiatives dans un temps plus long induit également leur évolution au sein d'un systeme économique et politique. Au final qu'est-ce que l'adoption par un plus large public de ces principes marginaux implique dans l'évolution du système politique et économique actuel ? Pour en arriver là, il faudrait d'abord voir en quoi la pérénnisation de telles initiatives permettrait de les sortir de leur statut marginale, pour les exposer à un public plus large.

Ainsi, d'autres questions socio-économiques se posent. Comment décider démocratiquement de la gestion des données et des informations, rôle qui incombait jusqu'à présent des organisations privées qui opéraient ces actions en interne sans réel droit de regard externe. S'émanciper des usages centralisés des GAFAM revient à endosser certaines responsabilités, de manière distribuée. Ainsi Alternet s'imposerait comme un ensemble de nouvelles pratiques politiques et économiques appliquées aux services numériques.


0x 63 0x 68 0x 65 0x
72 0x 63 0x 68 0x 65
0x 20 0x 73 0x 75 0x
72 0x 20 0x 77 0x 69
0x 6b 0x 69 0x 70 0x
65 0x 64 0x 69 0x 61
0x 20 0x 73 0x 69 0x
20 0x 74 0x 27 0x 61
0x 20 0x 64 0x 75 0x
20 0x 6d 0x 61 0x 6c

Nous avons vu au cours de cette recherche que les mécanismes d'annexion de notre vie privée sont utilisés sur le nouveau marché de la prédiction comportementale qui caractérise les services numériques du 21e siècle et du Web 2.0. En décorticant ces obscures machineries d'analyse, nous comprenons que l'utilisation de ces services provoque une forme d'accoutumance du fait de leur fluidité et leur facilité d'usage. Cependant, leur fonctionnement à l'éthique dorénavant questionnable, instrumentalise leurs utilisateurs, les transformant en matière première de l'économie du capitalisme de surveillance.

En réaction à cette annexion que subit notre vie privée, un ensemble de communautés alternatives émerge, que nous avons appelés Alternet, pour souligner leur désir de réapropriation de la technique au-delà des usages classiques et leur besoin de rendre possible des modes de vie furtifs au sein d'une société aux logiques de surveillance croissantes. Designers et développeurs se voient alors mobilisés sur ces divers fronts, qui réouvrent le champ des espaces, des collaborations et compétences par lesquels ils agissent sur les mondes socio-techniques.

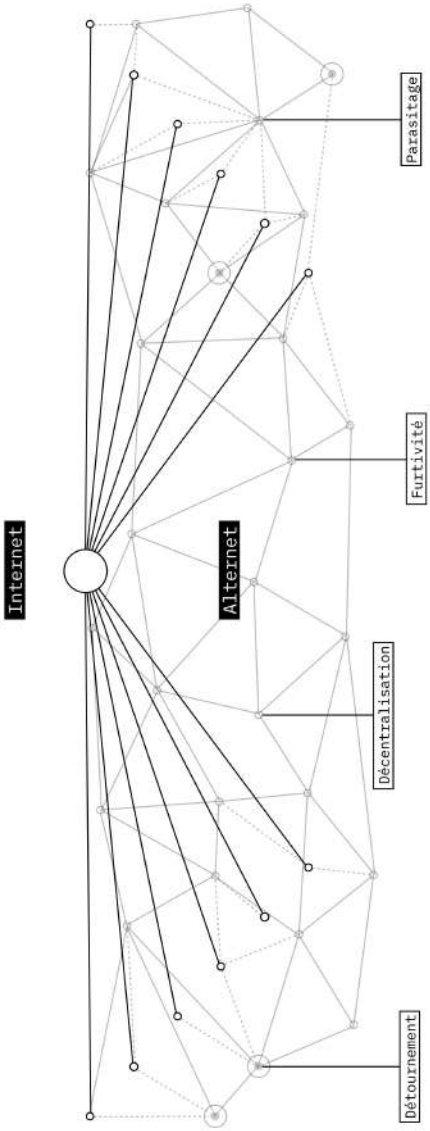
Sont-ils pour autant suffisamment reconnus ou valorisés pour les perspectives de basculement qu'ils initient ?

On peut en tout cas considérer qu'ils contribuent à ouvrir la voie et à légitimer des configurations de travail qui dépassent les cadres traditionnels de l'entreprise ou de l'institution publique. Depuis ces cadres de travail indépendants, insoumis aux politiques de captation des entreprises, les designers peuvent développer des systèmes induisant de nouveaux rapports d'usage à la technique : plus libres et distribués, se basant davantage sur la vérification des systèmes que sur la confiance à un tiers.

Ainsi, en instaurant de nouveaux modes de création "furtifs", les designers pourraient se donner pour rôle de distiller et diffuser la penser des cypherpunks : faire exister, au travers de dispositifs tangibles, des principes de furtivité numérique qui deviendront le support de nouveaux usages. Pour aller plus loin, il faudrait penser l'évolution dans le temps de ces dispositifs, de sorte qu'ils soient parasites, alternatifs, ou externes aux usages mis en place actuellement.

De ce fait, en faisant durer ces usages alternatifs, pensés selon une logique de pérennisation, on viendrait questionner l'utilité des algorithmes et des analyses comportementales du capitalisme de surveillance. Aujourd'hui malheureusement, ces logiques proches du sabotage sont pensées et mises en place en tant que dispositifs éphémères, justifiant par ce fait de continuer dans des usages centralisés classiques.

Ne serait-il pas temps de réaliser cet Alternet comme une série de dispositifs détournant les usages centralisés pour sa propre pérennité, remettant en cause de manière radicale et irrémédiable le fonctionnement maintennat obselette du Web 2.0.



Pastebin

Schema synthétique final de l'alternet

PastebinPastebinPastebinPastebinPastebinPastebinPa
stebinPastebinPastebinPastebinPastebinPastebinPast
ebinPastebinPastebinPastebinPastebinPastebinPasteb
inPastebinPastebinPastebinPastebinPastebinPastebin
PastebinPastebinPastebinPastebinPastebinPastebinPa
stebinPastebinPastebinPastebinPastebinPastebinPast
ebinPasteb tebinPasteb
inPastebin inPastebin

enîahc ednarg enu te emîba'l ed élc
al niam al à tianet lI .leic ud
erdnecsed egna nu siv ej siup

PastebinPastebinPastebinPastebinPastebinPastebinP**a**
stebinPastebinPastebinPastebinPastebinPas**t**ebinPast
ebinPastebinPastebinPastebinPastebinPastebinPasteb
inPastebinPastebinPastebinPastebinPastebinPastebin
PastebinPastebinPastebinPastebinPastebinPastebinPa
stebinPastebinPastebinPastebinPastebinPastebinPast
ebinPastebinPastebinPastebin**P**astebinPastebinPasteb
inPastebinPastebinPastebinPastebinPastebinPastebin
PastebinPastebinPastebinPastebinPastebinPastebinPa
stebinPastebinPastebinPastebinPastebinPastebinPast
ebinPasteb**in**PastebinPastebinPastebinPastebinPasteb
inPastebinPastebinPastebi**n**PastebinPastebinPastebin
PastebinPastebinPastebinPastebinPastebinPastebinPa
stebinPastebinPastebinPastebinPastebinPastebinPast
ebinPastebinPastebinPastebinPastebinPastebinPasteb
inPastebinPastebinPastebinPastebinPastebinPastebin
PastebinPastebinPastebinPastebinPastebinPastebinPa
steb**i**nPastebinPastebinPastebinPastebinPastebinPast
ebinPastebinPastebin**Pa**stebinPastebinPastebinPasteb
inPastebinPastebinPastebinPastebinPastebinPastebin
PastebinPastebinPastebinPastebinPastebinPastebinPa
stebinPastebinPastebinPastebinPastebinPastebinPast
ebinPastebinPastebinPastebinPastebinPastebinPasteb
inPastebinPastebinPastebinPastebinPastebinPastebin
PastebinPastebinPastebinPastebinPastebinPasteb

The Age of Surveillance Capitalism - Shoshana Zuboff : un ouvrage sur le thème de la surveillance de masse et son utilisation politique et commerciale rongeant l'évolution de la technologie actuelle.
https://bit.ly/3lrvTC2

Centre National de Ressources Textuelles et Lexicales
https://www.cnrtl.fr/

A Cypherpunk's Manisfesto - Eric Hughes : Le manifeste de la pensée Cypherpunk axée sur le droit à la vie privée et le contrôle de nos technologies par la libre circulation du savoir et le chiffrement.
https://activisme.fr/cypherpunk/manifesto.html

N-O-D-E : Réappropriation de matériel et création de dispositifs libres autour de la décentralisation et de l'open-hardware, une inspiration majeure pour mon choix de ce sujet.
https://n-o-d-e.net/

La societé de consommation - Jean Baudrillard page 32-33. https://bit.ly/3G36eYf

H A R V E S T - Julian Oliver : Un dispositif manifeste utilisant des éoliennes pour miner des cryptomonnaies qui seront reversées à des associations pour le climat, un travail manifeste qui remet en cause la création de valeur par l'utilisation de dispositifs alternatifs autonomes.
https://julianoliver.com/output/harvest

«Projet Pegasus» : Comment la société israélienne NSO a révolutionné l'espionnage. Le Monde, 19 juillet 2021 Le Monde, 19 juillet 2021.
https://www.lemonde.fr/projet-pegasus/article/2021/07/19/projet-pegasus-comment-la-societe-israelienne-nso-group-a-revolutionne-l-espionnage_6088692_6088648.html

Do We Need Wiretapping Laws? (1954) - débat TV entre deux sénateurs en ce qui cocnerne la légalisation de la mise sous écoute comme outils pour les forces de l'ordre en 1954. https://www.youtube.com/watch?v=IWsWWjFS0No

Disobedient Electronics. Garnet Hertz, Janvier 2018
https://www.disobedientelectronics.com/resources/Hertz-Disobedient-Electronics-Protest-201801081332c.pdf

Dead Drop - Aram Bartholl, octobre 2010. https://deaddrops.com/

Médiarchie - Yves Citton., pp. 939-340, citant Günther Anders, L'Obsolescence de l'homme, Paris, L'Encyclopédie des nuisances, 1956, p. 151, 155-156. https://libgen.is/book/index.php?d5=317AE8991CEFB582AEEE35BBFC85266E&tlm=2020-07-27%2003:48:31

Edward Snowden tweet - Twitter https://twitter.com/Snowden/status/975147858096742405?ref_src=twsrc%5Etfw

Online Mnipulation With Decision taking - Elena Boldyreva - pages 95 a 99. https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process

RGDP - https://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/es/pdf

What is the web 3.0 ? And why it matters ?
https://medium.com/fabric-ventures/what-is-web-3-0-why-it-matters-934eb07f3d2b

The TOR project - https://www.torproject.org/

Obfuscation, a user's guide for privacy and protest - Finn Brunton et Helen Nissenbaum
http://zkdppoahhqu5ihjqd4qqvyfd2bm4wejrhjosim67t6yopl77jitg2nad.onion/

QT scarf - Ceren Paydas - https://www.cerenp.com/q-t-scarf/

Backlash - Pedro G. C. Oliviera & Xuedi Chen - p 25-28
https://www.disobedientelectronics.com/resources/Hertz-Disobedient-Electronics-Protest-201801081332c.pdf

Critical Atlas Of The Internet, Spatial analysis as a tool for socio-political purposes Louise Druhle - https://louisedrulhe.fr/internet-atlas/

Les Furtifs - Alain Damasio - 2019

Priyom, forum communautaire d'écoute, d'enristrement et de documentation des number station.
https://priyom.org/about

Exemple de number station : https://priyom.org/media/152427/s06.ogg

Cryptii - Outils de Chiffrement et Cryptographie
https://cryptii.com/

Remerciements

Merci à toute l'équipe enseigante qui m'a accompagné tout au long de ce mémoire.

Merci à [redacted] pour ses conseils et l'aide conséquente sur la formulation.

Merci à [redacted] pour sa culture sans fin qui m'a aidé à nourrir ma reflexion.

Polices

Titrage - IBM plex mono
Texte - PP Fraktion mono
Obsidian - traitement de texte

OST

Phuture Doom - PHUTURE DOOM II
Phuture Doom - The Book Of Nightfall
Perturbator - “New model”
VY1 & VY2 - サイバーサンダーサイダー
VY1 & VY2 - とても痛い痛がりたい
Two-Mix - Just Communication
Wulfband - Wulfband
Massive Attack - Mezzanine
Master Boot Record - Internet Protocol
Keygen Church - S E V E R K E T O R
LORN - The Maze To Nowhere
The Algorithme - Bruteforce
IAH - III
AXIOM9 - Space Debris
Hiroyuki Sawano - Unicorn

解决方案列在所有页面上