SURVIVALISME NUMERIQUE EN ZONE URBAINE HOSTILE

Vous avez tous lu ou entendu parler du livre 1984 où Big Brother se servait du Telecran pour surveiller tout le monde par l'intermédiaire d'un écran de télévision. Le héros avait trouvé un angle mort dans son logement pour lui permettre d'échapper à la surveillance des autorités. C'est de la science-fiction, puisqu'un téléviseur ne permet pas cela, mais c'est désormais devenu possible avec nos outils de communication actuels, qui sont connectés dans les deux sens, de l'émetteur vers l'utilisateur et inversement de l'utilisateur vers un service central. Se soustraire à la surveillance numérique nécessite une posture, un comportement vigilant par rapport à nos appareils, et c'est cette posture que je vous propose d'envisager, en regardant comment sont conçus nos appareils pour générer différentes techniques de surveillance, et détecter leurs failles.

J'ai été très jeune inspiré par cette manière de considérer la situation, alors que sous les drapeaux, j'ai été intégré à une cellule de guerre électronique. J'ai eu ainsi plusieurs fois l'occasion d'observer comment les sous-marins se préparent à attaquer les navires de guerre, en émettant très brièvement sur des radars de chalutiers pour se situer dans leur environnement et trouver leurs cibles. Ils pointent ensuite leur radar de tir sur celle qu'ils ont choisie, mais c'est trop tard pour le porte-avions ou la frégate qui l'accompagne ! La furtivité n'est pas seulement déterminée par la technique, mais aussi par un comportement, une posture qui va déjouer des adversaires.

1. Mon IP est mon identité
    - IP = Internet Protocol, IP fixe et dynamique ;
    - Les réseaux sociaux, « l'homme du milieu » ;
    - VPN, Tor, messageries cryptées, mail ;

2. L'adresse MAC

3. Le téléphone mobile, un super-Minitel
    - L'expérience désastreuse de l'ETA
    - Le *smartphone*, un outil de surveillance itinérant :

Dans cette séance, nous découvrons les ressources insoupçonnées de nos *smartphones* pour appréhender notre environnement numérique, nous commençons ensuite à espionner les autres grâce à leur identité numérique qui nous est indiquée sur nos appareils.

Nous sortons de la salle, formons une ronde et nous les rallumons. Un premier exercice consiste à chercher l'adresse MAC de la carte réseau dans les paramètres de l'appareil : c'est notre nouvelle identité, celle qui va nous identifier sur les réseaux.

Puis, nous activons le Bluetooth et nous nous reconnaissons les uns, les autres, parmi les adresses MAC et les noms des machines qui viennent à apparaître sur l'écran. Nous réitérons la même opération en activant le Wi-Fi. Nous découvrons une multitude d'appareils supplémentaires, ceux des habitants de la résidence. Les fréquences radio du Bluetooth sont comprises entre 2,4 et 2,483 GHz, soit une longueur d'onde de 12,5 cm. Sa portée ne va pas dépasser 33 pieds soit 10 mètres. Le Wi-Fi utilise aussi les 2,4 GHz, mais parfois aussi deux de l'ordre 5 GHz. Sa portée est inférieure à 100 mètres, et optimale entre 30 et 50 mètres.

Nous essayons alors de nous connecter à l'un de ces appareils, il nous demande un login et un mot de passe que nous ignorons et ne pouvons pas fournir.

Nous sortons ensuite dans la rue, et essayons d'identifier un passant grâce à son signal Bluetooth, lequel va apparaître dans la liste des appareils situés dans notre environnement immédiat. Dès qu'il nous semble avoir vu un nouvel appareil, un binôme se détache du groupe pour essayer de suivre son détenteur. Nous découvrons ainsi une nouvelle manière d'exercer une filature — via son identité numérique — et sans jamais poser une seule fois les yeux sur la personne !

4. Le passe sanitaire, porte d'entrée du crédit social
    - Comment nos vies sont volées ;
    - L'espace de santé numérique ;
    - L'expérience du prélèvement à la source ;
    - Le portefeuille digital de Thales ;

5. Les caméras vidéo de surveillance
    - La numérisation de l'espace public à comparer à celle du champ de bataille ;
    - Les failles techniques et les postures à adopter ;

6. L'effet boomerang de la vidéo témoignage

7. Les voisins, les badauds, témoins gênants

On parle depuis la guerre froide des conflits asymétriques, opposant des groupes armés de bric et de broc aux armées des grandes puissances. Mais ce n'est pas un phénomène nouveau. La guerre de partisans, en URSS et dans de nombreux pays européens sous la domination nazie ont été soutenus par l'arrière du front en Russie, et depuis l'Angleterre (SOE) ailleurs en Europe. La Résistance française a été pratiquement détruite par l'Abwehr et la Gestapo à l'hiver 1943-44, par des moyens techniques (gonio), mais aussi humains. Nos gouvernements semblent tellement aveuglés par la technique qu'ils en oublient les moyens humains, c'est une opportunité qu'il convient de ne pas négliger pour vaincre, et ce ne serait que justice puisque nous ne voulons pas adhérer à une société où l'humain est négligé, où la machine est là pour nous dominer… Les conflits asymétriques finissent en général par le triomphe du faible sur le fort, et c'est le sens que nous a donné l'histoire de David contre Goliath dans la Bible. Mais il est nécessaire pour hâter la fin de reprendre la main sur la machine !

RESSOURCES WEB :

https://fr.wikipedia.org/wiki/Dr%C3%B4le_de_jeu
https://www.lesechos.fr/politique-societe/societe/lespace-de-sante-numerique-sera-deploye-pour-tous-le-1er-janvier-annonce-olivier-veran-1356150
https://www.polemia.com/passe-sanitaire-credit-social-a-la-chinoise-thales-au-coeur-de-la-societe-de-surveillance/
https://francais.rt.com/international/92665-italie-perquisitions-chez-anti-pass-sanitaire-accuses-planifier-actions-violences
https://myip.ms/
https://www.techno-science.net/definition/1433.html
https://invidious.fdn.fr/watch?v=uJY8nWdLQn4

ANNEXES


COVID-19 PASSPORT
PASSEPORT COVID-19
NAME
JOHN DOE
ID
ISSUED
05/22/2021
REISEPASS
PASSPORT


Carnet
FR
MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
HUAWEI