EPFL

Thèse n° 8838

Opacité et transparence dans le design d'un dispositif de surveillance urbain : le cas de l'IMSI catcher

Présentée le 7 juillet 2022

Collège des humanités
Laboratoire d'humanités digitales
Programme doctoral en architecture et sciences de la ville

pour l'obtention du grade de Docteur ès Sciences

par

Félicien Michel Marie GOGUEY

Acceptée sur proposition du jury

Dr J. Chenal, président du jury
Prof. F. Kaplan, Dr N. Nova, directeurs de thèse
Dr L. Allard, rapporteuse
Dr E. Quinz, rapporteur
Dr J. Baudry, rapporteur

École
polytechnique
fédérale
de Lausanne

2022

Opacité et transparence dans le design d'un dispositif de surveillance urbain : le cas de l'IMSI catcher

Thèse présentée à l'école doctorale de l'EPFL dans le programme Architecture et sciences de la ville en partenariat avec la HEAD – Genève par Félicien Goguey, le 25 octobre 2021, sous la direction de Frédéric Kaplan et de Nicolas Nova pour l'obtention du grade de docteur ès sciences.

Membres du jury de thèse :
Frédéric Kaplan, directeur de thèse (EPFL)
Nicolas Nova, directeur de thèse (HEAD – Genève)
Jérôme Chenal, président du jury (EPFL)
Jérôme Baudry (EPFL)
Laurence Allard (Université de Lille - IRCAV)
Emanuele Quinz (Université Paris 8)

Résumé

Cette thèse s'intéresse à la surveillance opérée sur le réseau téléphonique mobile par les acteurs gouvernementaux (agences de renseignement, police, armée) et aux rapports entre les espaces surveillés et les usagers de ceux-ci. En effet, de nouveaux dispositifs utilisés par les services de renseignement redéfinissent les espaces de surveillance et posent de nouvelles interrogations dans ce champ de recherche. Plus spécifiquement, ce travail se concentre sur un objet de la surveillance : l'IMSI catcher, un appareil de surveillance du réseau téléphonique mobile qui intercepte l'identité des téléphones et certaines communications dans une zone donnée en se faisant passer pour une antenne relais. Si ce type de dispositif semble présenter un intérêt tactique et sécuritaire dans la lutte anti-terroriste et anti-criminelle, de nombreuses organisations de défense des libertés sur les réseaux telles que EFF, Privacy International ou la CNIL mettent en garde face à une éventuelle surveillance incontrôlée ; ainsi, la nature controversée du dispositif pourrait mettre en péril certaines libertés individuelles et publiques. Quel est cet objet technique et quels nouveaux enjeux apparaissent avec son utilisation dans la surveillance ? En quoi et depuis quelles perspectives celui-ci est-il problématique ? Qu'est-ce que l'IMSI catcher nous apprend sur le futur potentiel des régimes de surveillance ? Je me penche sur le cas de ce dispositif dans un cadre de recherche à l'intersection de pratiques de recherche en design, des études des sciences et technologies (STS) et des *surveillance studies*. Dans un premier temps, je m'intéresse à l'avènement de cet appareil de surveillance en tant qu'objet technique depuis une perspective nourrie par le cadre théorique de la concrétisation et des lignées techniques proposé par Gilbert Simondon et Yves Deforge, et ce à partir de l'analyse d'une documentation visuelle et technique. Dans un second temps, j'emploie une démarche de recherche-création pour explorer certaines hypothèses quant à la nature même de l'objet, son fonctionnement et son aspect « concret » — ou plutôt « non-concret » dans le cas présent — à l'aide de démarches empruntées à la rétro-ingénierie, à la reconstitution et proches de l'archéologie des médias. Puis, j'explore des trajectoires d'opposition et de protestation possibles à l'aide de prototypes conçus à partir de méthodes issues du design critique et du design spéculatif. Enfin, à travers l'écriture de scénarios prospectifs, je construis une *design fiction* qui propose une synthèse, objet potentiel de débats, autour des usages présents et à venir de l'IMSI catcher et plus globalement sur le devenir potentiel des régimes de surveillance.

Mots-clés : *surveillance, contre-surveillance, réseau, téléphonie mobile, IMSI catcher, design critique, design spéculatif, design fiction, critical making, interaction*

Abstract

This thesis assesses the surveillance operated on the mobile phone network by governmental actors (intelligence agencies, police, army) and the relationship between monitored spaces and their users. Indeed, some new surveillance devices used by intelligence services redefine surveillance spatiality raising new questions in this field of research. More specifically this research focuses on one specific object: the IMSI catcher, a monitoring apparatus of the cellular network that intercepts cellphones' identity and some communications in a given area by mimicking the activity of a cell tower. While this kind of device seems to offer a tactical and a security interest in the fight against terrorism and against crime, many civil liberties organisations such as the Electronic Frontier Foundation, Privacy International and *La Commission nationale de l'informatique et des libertés* are concerned about the potential of an uncontrolled surveillance ; indeed, the controversial nature of the device could endanger certain individual and public rights. What is this technical object and which new issues comes with its use in surveillance? How and from which perspective is it problematic What does the IMSI catcher teaches us on the potential future of surveillance regimes? I look into this specific device case in a research framework at the intersection of design research practices, science and technology studies (STS) and surveillance studies. First, I deal with this surveillance apparatus as a technical object, from a perspective fed by the theoretical framework of *concretization* and *technical lines* proposed by Gilbert Simondon and Yves Deforge, through the analysis of a visual and technical documentation. Second, I use a research by design approach to explore certain assumptions regarding the nature of the object itself, its functioning and its "concrete" aspect – or rather "non-concrete" in the present case – with the help of approaches borrowed to reverse engineering and reconstitution, close to media archeology. Then, I explore possible opposition and protest trajectories with the help of prototypes designed with critical design and speculative design methods. Finally, through the writing of prospective scenarios, I build a design fiction that offers a synthesis, potentially subject to debate, around the IMSI catcher's uses, present and to come, and more broadly on the potential future of surveillance regimes.

Keywords : *surveillance, counter surveillance, network, mobile phone, IMSI catcher, critical design, speculative design, design fiction, critical making, interaction*

1 **Introduction** **10**
1.1 IMSI catcher, *Stingray*, *Dirtbox* ? 12
1.2 Un objet controversé 14
1.3 Un objet (il)légal 15
1.4 Un objet opaque 16
1.5 Recherche-création 20

2 **État de l'art** **22**
2.1 Du panoptique aux *surveillance studies* 23
2.2 Surveillance algorithmique 27
2.3 Surveillance électromagnétique 32
2.4 Surveillance téléphonique mobile 38
2.5 Surveillance studies et pratiques de recherche en art et en design 41

3 **Cadre théorique et méthodologique** **44**
3.1 Recherche sur le design 49
3.2 Recherche par le design I : Reconstitution 54
3.3 Recherche par le design II : Prototypes 56
3.4 Recherche par le design III : Scénarios 63

4 **Recherche sur le design : Étude d'un objet confidentiel** **68**
4.1 Vers une typologie ? 70
4.2 Des composants de l'IMSI catcher 73
4.3 Du caractère non-concret de l'IMSI catcher et de la pertinence de la reconstitution 74

5 **Recherche par le design I : Refaire un IMSI catcher** **100**
5.1 Le processus de reconstitution 101
5.2 De la pertinence de reconstituer le présent 110
5.3 Mythes et spéculation 113
5.4 Vers la constitution d'une boîte à outils 114
5.5 Produire à partir de la reconstitution : *900 MHz* 115

6 **Recherche par le design II : Vers des objets de contestation** **136**

6.1 Des objets de contestation 137

6.2 Workshop *900 MHz: Protest* 139

6.3 *BlocBalloon* : concevoir un objet de contestation contre la surveillance du réseau GSM 159

6.4 Du rôle des objets désobéissants 172

7 **Recherche par le design III : Vers le design fiction** **178**

7.1 Construction des scénarios 179

7.2 Scénarios prospectifs 182

8 **Discussion & conclusions** **206**

8.1 Un objet au statut particulier 207

8.2 Code, espace et opacité 211

8.3 Contre-surveillance et contre-mesures 214

Bibliographie **218**

Remerciements **228**

1
Introduction

Au cours des années 2010, plusieurs articles de presse ont relaté la survenance d'interactions étranges avec des téléphones portables notamment lors de manifestations. Ainsi, *The Guardian*[1] rapporte en 2013 l'envoi de messages en masse aux participants d'une manifestation pro-européenne à Kiev en Ukraine, à l'encontre du président prorusse Viktor Ianoukovytch. Les manifestants, ainsi que les personnes munies d'un téléphone portable aux alentours de la manifestation, ont reçu simultanément les messages suivants : « *Dear subscriber, you are registered as a participant in a mass riot* ». Les opérateurs téléphoniques MTS et Kyivstar réfutaient cependant être à l'origine de l'envoi de ces messages, les soupçons se sont alors tournés vers le gouvernement en place et les forces de l'ordre qui auraient pu procéder de la sorte via l'utilisation d'antennes relais pirates. Cette manière de procéder suggère l'utilisation d'un dispositif à même d'exploiter les failles du réseau téléphonique mobile, une fonction portée par un objet dédié : l'IMSI catcher.

Lors des manifestations Black Lives Matter de 2014, des images d'appareillages inhabituels montés sur des véhicules d'intervention suscitaient l'interrogation sur les réseaux sociaux (Twitter)[2]. De la même façon, certains internautes relataient le survol d'autres manifestations Black Lives Matters de 2020 par des avions qui auraient embarqué des IMSI catchers afin de surveiller l'activité des manifestants au sol[3].

Plus récemment, le chercheur en design et humanités numériques Jason Farman (2016) mentionnait un rapport de presse titrant « *Mysterious Phony Cell Towers Could be Intercepting Your Calls* »[4] qui relatait l'existence d'antennes relais factices sur le territoire états-unien ; celles-ci interceptaient les données des téléphones mobiles qui s'y connectaient avant de transférer leurs appels au réseau « authentique », reposant ainsi sur le principe de l'attaque de l'homme du milieu. Les articles de journaux publiés autour de ce phénomène provoquaient une part de spéculation quant aux auteurs de ces actions, depuis des organisations terroristes aux instances gouvernementales en passant par des cartels de drogues ou encore des entreprises privées accusées d'espionnage industriel.

Dans le champ académique, Lisa Parks chercheuse en *media studies* rapportait des cas d'espionnage industriel conduits à l'aide d'IMSI catchers notamment en Inde (Parks, 2016). D'après elle, des entreprises privées auraient fait passer 2000 IMSI catchers (fabriqués en Israël, en Chine, au Royaume-Uni en France et en Suède)

1 <https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot> consulté le 15.02.2022

2 <https://inthesetimes.com/article/a-slip-of-an-officers-tongue-suggests-police-are-monitoring-ferguson-protes> consulté le 15.02.2022

3 <https://www.vice.com/en/article/y3zvwj/military-fbi-flying-surveillance-planes-george-floyd-protesters> consulté le 15.02.2022

4 <https://www.businessinsider.com/mysterious-fake-cellphone-towers-intercept-calls-2014-9?IR=T> consulté le 15.02.2022

aux frontières du Bangladesh et du Népal, et les auraient utilisé pour intercepter des conversations téléphoniques mobiles. Ces IMSI catchers auraient été importés en majorité par le secteur privé. Bien qu'ayant été bannis par le gouvernement indien en 2012, les IMSI catchers jouent un rôle prépondérant dans la culture entrepreneuriale extrêmement compétitive en Inde où les entreprises tirent parti de son avantage stratégique dans l'espionnage de la concurrence. En dehors des travaux de Farman et Parks, peu de travaux académiques dans le champ de la surveillance, des *media studies* et du design s'intéressent au cas de l'IMSI catcher et laisse ce champ de recherche relativement inexploré ; et ce, alors qu'il offre une opportunité d'aborder le thème des technologies de surveillance avec un regard nouveau.

Ainsi, dans cette thèse, je m'intéresse à la surveillance opérée sur le réseau téléphonique mobile par les acteurs gouvernementaux (agences de renseignement, police, armée) et aux rapports entre les espaces surveillés et les usagers de ceux-ci. En effet, les récents dispositifs utilisés par les services de renseignement redéfinissent les espaces de surveillance et posent de nouvelles interrogations dans ce champ de recherche. Je focalise ma recherche autour d'un objet d'étude : l'IMSI catcher, un appareil de surveillance du réseau téléphonique mobile qui intercepte l'identité des téléphones et les communications dans une zone donnée en se faisant passer pour une antenne relais.

1.1 IMSI catcher, Stingray, Dirtbox ?

L'IMSI catcher étant un objet technique[5] numérique, il est tout d'abord nécessaire de définir certains aspects techniques sur lesquels il repose. En effet, l'IMSI catcher utilise des failles de la norme GSM à des fins d'interception et de surveillance et repose sur l'attaque dite de « l'homme du milieu ».

Si le terme numérique s'appliquait plutôt auparavant à toute information interprétable en nombre, quantifiable et calculable, les technologies numériques désignent aujourd'hui plus largement les technologies et de l'information et de la communication. Le standard GSM (pour *Global System for Mobile Communications*) qui en fait ainsi partie est introduit au cours des années 1990. Il est principalement utilisé dans les réseaux d'appellation commerciale dite 2G (correspondant à la seconde génération des standards de communication mobile) et exploite les gammes de fréquences des 900 MHz et 1800 MHz en Europe. Ainsi, cette norme de communication, comme toute communication sans fil, utilise le rayonnement électromagnétique pour fonctionner. Pour pouvoir l'étudier, ce rayonnement électromagnétique est le plus souvent représenté par des ondes électromagné-

5 Objet produit et manipulable par l'Homme dans un but utilitaire, mais qui a sa propre existence individuelle dans le sens d'organisme non-vivant selon Simondon.

tiques : c'est le cas des ondes lumineuses (autrement dit la représentation des rayonnements visibles), des ondes infrarouges, des micro-ondes et dans notre cas des ondes radio. Toutes ces ondes sont classées sur le spectre électromagnétique en fonction de leur longueur et de leur fréquence ; certaines bandes de fréquences radio du spectre sont réservées à des protocoles donnés ou à des domaines spécifiques comme l'armée ou l'aérospatiale, tandis que d'autres sont utilisables par le grand public. Nous verrons plus loin en quoi la dimension électromagnétique de l'objet étudié renforce son caractère opaque.

Historiquement, en Europe, le dispositif étudié est d'abord commercialisé par l'entreprise allemande Rhodes & Schwartz sous le nom de « IMSI catcher » et dont la première implémentation remonte à 1993. Ce nom vient du fait que la principale action du dispositif consiste à intercepter l'IMSI pour *International Mobile Subscriber Identity*, un identifiant unique associé à la carte SIM et qui permet au réseau téléphonique mobile d'identifier un usager[6]. Son homologue américain est commercialisé par Harris Corporation sous le nom de Stingray dans les années 2000[7]. Ainsi, dans le monde anglo-saxon *Stingray* est devenu un terme générique pour désigner l'objet étudié. Toujours dans la sphère anglo-saxonne, il existe aussi l'appellation *Dirtbox* de l'entreprise qui la commercialise (DRT pour Digital Receiver Technology, Inc.) et on relève souvent le terme *cell-site simulator* que l'on peut grossièrement traduire par « simulateur de cellule » (comprendre simulateur d'antenne relais). Il existe donc une multitude de dénominations pour un objet dont le principe de fonctionnement est en substance le même, si l'on exclue sa forme et son contexte d'utilisation. Le dispositif étudié dans cette thèse sera le plus souvent désigné sous la dénomination d'IMSI catcher.

Fig.1 Composition de l'IMSI.

6 L'IMSI est en fait composé du MCC (*Mobile Country Code*), du MNC (*Mobile Network Code*) et du MSIN (*Mobile Subscriber Identification Number*), en d'autres termes : l'identifiant du pays d'origine (par exemple 228 pour la Suisse, 208 pour la France), l'identifiant de l'opérateur téléphonique mobile (par exemple en Suisse, 01 pour Swisscom, 02 pour Sunrise, 03 pour Salt) et l'identifiant de la carte SIM (associée à son utilisateur et à un numéro de téléphone).

7 <https://www.wired.com/2014/03/stingray/> consulté le 15.02.2022

1.2 Un objet controversé

Outre les controverses sociales rapportées dans les médias évoquées plus haut, on peut constater que différents points de vue expriment le caractère controversé de l'IMSI catcher, notamment ceux des associations mais aussi de certains organismes publics de protection de la vie privée.

Ainsi, certaines associations de défense des libertés individuelles comme EFF, Privacy International ou encore la Quadrature du Net mettent en garde face au caractère intrusif et indétectable de ce dispositif ainsi que face à son mode opératoire « coup de filet » — drag net en anglais, en ce sens que le dispositif collecte les données de tous les téléphones dans son rayon d'action, et ce sans aucun filtre. Ainsi, dans son commentaire à l'article 21 de l'International Covenant on Civil and Political Rights (ICCPR), Privacy International (2019) consacre un paragraphe au cas de l'IMSI catcher[8], qui pour eux est une menace au droit au respect de la vie privée et à la liberté d'expression, mais aussi à la liberté de réunion. En 2012, l'Electronic Frontier Foundation[9] émettait déjà un avertissement à propos de « la plus grande menace technologique vis-à-vis du respect du droit à la vie privée sur le réseau téléphonique mobile » que représentaient les *Stingrays*. Notamment parce que lorsqu'ils sont utilisés par la police, ceux-ci n'interceptent pas uniquement les données des suspects, mais aussi de toutes les personnes présentes dans la zone d'émission qui peut s'étendre sur plusieurs kilomètres dans certains cas, ainsi les *Stingrays* collecteraient les données de « centaines de personnes innocentes » voyant leur droit à la vie privée enfreint sans être suspecté d'aucun délit. De la même manière, la CNIL[10] en France émettait un rapport d'une délibération portant avis sur le projet de loi relatif au renseignement 2015 qui visait entre autres à légaliser l'utilisation « de dispositifs techniques de proximité (dits *IMSI catchers*) », et soulignait la nécessité d'un cadre légal qui limite au strict nécessaire les atteintes portées au respect de la vie privée[11]. Dans le contexte Suisse, un autre exemple de controverse est issu d'une interpellation de la Direction de la police et des affaires militaires du canton de Berne (2016), dans laquelle un membre du Grand Conseil s'inquiète du recours à l'IMSI catcher par la police bernoise et du danger que cela représente vis-à-vis de la protection des données[12].

8 <https://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle21/PrivacyInternational.pdf> consulté le 15.02.2022

9 <https://www.eff.org/fr/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy> consulté le 15.02.2022

10 La Commission nationale de l'informatique et des libertés de France est une autorité administrative indépendante française.

11 <https://www.cnil.fr/sites/default/files/typo/document/D2015-078-PJLRenseignement.pdf> consulté le 15.02.2022

12 <https://www.gr.be.ch/etc/designs/gr/media.cdwsbinary.DOKUMENTE.acq/93cd78b9aa4e4bef8fb2fc568cdd011e-332/2/PDF/2015.RRGR.1037-GR-Wortlautdokument-F-136432.pdf> consulté le 15.02.2022

Si ce type de dispositif semble présenter un intérêt tactique et sécuritaire dans la lutte anti-terroriste et anti-criminelle, on peut toutefois se poser la question d'une éventuelle surveillance incontrôlée. En effet, comme nous l'avons vu précédemment, l'IMSI catcher intervient sur les données de tous les téléphones présents dans son champ d'action. Aussi, si ces controverses s'inscrivent dans la prolongation d'autres controverses liées à des dispositifs de surveillance précédents (caméras de surveillances par exemple) ; celles-ci soulignent de nouveaux enjeux, notamment liés à la mobilité, à la portée et à l'opacité du dispositif sur laquelle je reviendrai plus tard. Enfin, plusieurs rapports budgétaires et parlementaires comme on va le voir maintenant font état d'une mise à disposition et d'une utilisation par certaines forces de l'ordre alors que le dispositif ne faisait à l'époque l'objet d'aucun cadre légal, cadre légal qui a depuis évolué.

1.3 Un objet (il)légal

Si l'on s'intéresse uniquement aux contextes suisse et français, afin de contourner le problème de dénomination de l'IMSI catcher énoncé précédemment, les textes de loi s'attachent à décrire le but du dispositif utilisé plutôt que son fonctionnement lui-même et permettent l'utilisation des IMSI catchers mais aussi d'autres dispositifs qui auraient la même finalité d'action. Ainsi, en Suisse, le Code de procédure pénale autorise « d'écouter ou d'enregistrer des conversations, ou d'identifier ou de localiser une personne ou une chose » (Art. 269bis1 du Code de procédure pénale suisse du 5 octobre 2007)[13]. De la même manière en France la Loi sur le renseignement adoptée en 2015, après les attaques terroristes de Charlie Hebdo décrit un « dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet » (Art. L. 851-5. LOI n° 2015-912 du 24 juillet 2015 relative au renseignement) et permet l'« utilisation d'un appareil ou d'un dispositif technique [...] afin d'intercepter des correspondances émises ou reçues par un équipement terminal » (Art. L. 852-1.-II. LOI n° 2015-912 du 24 juillet 2015 relative au renseignement).

Toutefois, l'IMSI catcher fait son apparition dans des budgets publics (des douanes françaises notamment) avant la légalisation de son usage. Ainsi, Le Monde[14] en 2015, en se basant sur un rapport budgétaire de la Direction nationale du

13 À l'exception des autorités compétentes, l'utilisation d'un IMSI catcher à des fins de surveillance de la correspondance est illégale en Suisse. C'est pourquoi dans le cadre de cette recherche, dès juin 2018, je me suis adressé à Sylvain Métille, avocat spécialiste de la protection des données et de la sphère privée et professeur de droit, criminalité et sécurité des technologies de l'information à l'Université de Lausanne, afin d'inclure la perspective juridique dans l'objectif et la méthodologie générale de la thèse et de me prémunir de problèmes éventuels.

14 <https://www.lemonde.fr/pixels/article/2015/05/20/les-douanes-ont-achete-des-imsi-catchers-alors-que-leur-utilisation-est-illegale_4636988_4408996.html> consulté le 15.02.2022

renseignement et des enquêtes douanières (DNRED) daté de 2014, mentionne une transaction de 30 000 euros avec l'entreprise française Amesys pour l'« acquisition d'un IMSI catcher miniature ». De la même manière, le document recensant l'attribution des marchés publics de la DNRED en 2012 mentionne la « transformation de l'IMSI-catcher en système autonome avec son amplificateur de puissance » pour une somme de 187 947 euros déboursée auprès de l'entreprise Nethawk. D'autres transactions de la même nature apparaissent dès 2010 et posent la question de l'usage illégal d'un tel dispositif par les douanes mais aussi par d'autres services de renseignement.

En outre, des doutes ont été émis par la Quadrature du Net sur une potentielle utilisation d'IMSI catcher lors de la votation de la Loi sur le renseignement de 2015[15] puisque certains membres de l'association ont pu constater l'apparition d'anomalies sur le réseau pouvant suggérer la présence d'IMSI catchers, fait marquant étant donné que ledit texte de loi visait en partie à légaliser l'utilisation de tels dispositifs d'interception. Néanmoins, pour Adrienne Charnet porte-parole de la Quadrature du Net il faut faire preuve de prudence puisque les preuves n'étaient pas suffisantes pour affirmer de manière certaine la présence d'IMSI catchers à ce moment[16].

On peut ainsi constater à travers les controverses qui l'entourent ainsi qu'à travers le flou juridique qui l'a entouré que l'IMSI catcher est un objet qui suscite de nombreuses interrogations, notamment vis-à-vis des nouveaux enjeux qui apparaissent avec son utilisation à des fins de surveillance. Se pose aussi la question des craintes qu'il suscite du côté des personnes surveillées et de l'exploitation des données collectées par de tels systèmes. Enfin, cet objet est relativement peu étudié dans le champ académique, que ce soit dans les *surveillances studies*, dans les études des sciences et des technologies ou d'un point de vue de son design. Pour ce faire, il convient de s'intéresser à la technicité et à l'opacité de cet objet.

1.4 Un objet opaque

L'une des caractéristiques les plus remarquables de l'IMSI catcher est son opacité. Celle-ci découle de plusieurs facteurs ; tout d'abord de son mode d'action : pour le propriétaire d'un téléphone, il n'y a pas (ou presque) de moyens de savoir qu'il est placé sous surveillance, puisque l'appareil surveillé donne des informations de connexion identiques à celles qu'il donnerait s'il était sur un réseau établi appartenant à un opérateur mobile connu. En effet, comme mentionné plus haut

15 <https://www.francetvinfo.fr/politique/loi-renseignement-des-imsi-catcher-espions-devant-l-assemblee_1691299.html> consulté le 15.02.2022

16 <https://www.nouvelobs.com/rue89/rue89-police-justice/20150416.RUE8695/devant-l-assemblee-des-valises-espionnes-pas-assez-de-preuves.html> consulté le 15.02.2022

l'IMSI catcher repose sur une technique bien décrite dans la littérature de la sécurité informatique, la technique dite de l'attaque de l'homme du milieu — *man-in-the middle attack* en anglais : l'attaque dite de « l'homme-du -milieu » consiste à intercepter et/ou modifier une communication entre un émetteur A et en récepteur B sans qu'aucun des deux aie le moyen de vérifier si le message a été intercepté et/ou modifié. L'intercepteur C se place ainsi entre les deux parties communicantes A et B sans que celles-ci puissent s'apercevoir que le canal de communication établi entre elles a été compromis. Ce type d'attaque est largement utilisée sur Internet (pour l'interception d'emails ou de données privées) et dans les communications sans fil (GSM notamment).

En outre, l'IMSI catcher tire parti d'une certaine opacité de l'objet lui-même. Premièrement d'une opacité physique : comme nous avons pu le voir précédemment, l'IMSI catcher intervient dans une partie du spectre électromagnétique, ce qui participe à son caractère opaque. Son action intervient dans l'espace hertzien qui n'est pas perceptible ou visible sans l'utilisation d'outils adéquats, il n'est donc pas possible pour l'utilisateur de voir quel type d'action est conduit dans cet espace. Aussi, dans le cas spécifique de la téléphonie mobile, l'utilisateur en déplacement transite sans cesse d'une cellule[17] à une autre de manière tout à fait fluide, phénomène complètement imperceptible pour l'utilisateur : si celui-ci était amené à rencontrer un IMSI catcher (qui simule l'activité d'une antenne-relai), il n'en serait pas informé.

De plus, le dispositif revêt une opacité d'une autre nature, qui repose plutôt sur un processus d'invisibilisation dans sa conception. En effet, l'IMSI catcher a été conçu comme une « boîte noire »[18] — ou « boîte opaque ». Cette notion de boîte noire est théorisée pour la première fois dans le champ de la cybernétique par Norbert Wiener (1948) comme un objet dont on connait l'entrée et la sortie, mais pas le fonctionnement interne. Dans le champ de la sociologie et des sciences des techniques (STS), la notion de « black box » est d'autant plus pertinente à l'égard de notre objet d'étude ; Dominique Vinck en propose la définition suivante :

> « Le terme de boîte noire est issu de la cybernétique où il désignait une partie de l'appareil dont on ne connait rien de la mécanique interne mais seulement l'entrée et la sortie. Il est utilisé en sociologie des sciences pour parler d'un fait ou d'un artefact technique bien établi. Il signifie que l'outil ne fait plus l'objet de controverse, d'interrogation, ni de doute mais qu'il est pris comme un donné ou un acquis. Cela signifie parfois qu'on en ignore ou qu'on en a oublié le fonctionnement interne. L'opacité de la boîte noire tient au fait que les mécanismes

17 Zone couverte par une antenne relais.

18 Comme elle est définie dans la cybernétique et non pas dans l'aéronautique où elle consiste en fait en deux boîtes oranges qui enregistrent respectivement l'activité sonore dans le cockpit d'un avion et les actions des pilotes.

> internes sont articulés entre eux d'une manière si verrouillée qu'il est difficile pour un utilisateur non-outillé de les remettre en cause (...) l'utilisateur est rendu particulièrement dépendant de ceux qui les ont conçues. » (Vinck, 1995, p.176)

Ainsi, dans le cas des réseaux de téléphonie mobile, l'utilisateur n'a pas à connaître les protocoles de communication à l'œuvre pour passer un appel ou envoyer un SMS : le téléphone mobile et le système socio-technique autour de lui (le réseau, les choix de protocoles de communication, etc.) est en ce sens une boîte noire. Les chercheurs en STS y voient plus largement un processus social qu'il nomment « black boxing » (« fermeture de la boîte noire ») d'après le sociologue et philosophe des sciences Bruno Latour comme :

> « the way scientific and technical work is made invisible by its own success. When a machine runs efficiently, when a matter of fact is settled, one need focus only on its inputs and outputs and not on its internal complexity. Thus, paradoxically the more science and technology succeed, the more opaque and obscure they become. » (Latour, 1999, p.304)

Il faut comprendre ici que lorsqu'une machine fonctionne de manière suffisamment efficace, elle change de nature et subit une transformation : il n'est plus nécessaire de connaitre son fonctionnement interne pour l'utiliser, elle passe d'objet technique à boîte noire. Latour est rejoint sur ce point en particulier par la sociologue Madeleine Akrich :

> « La transformation de faits socio-techniques à des faits tout courts passe donc par la transformation de l'objet technique en boîte noire: il s'efface dans le même temps qu'il est plus indispensable que jamais. » (Akrich, 1987, p.13)

Dès lors, on comprend que l'opacité des objets techniques, et en particulier de l'IMSI catcher, ne repose pas uniquement sur l'opacité physique, mais aussi (et surtout) sur une opacité liée à son processus de conception même. En outre, dans ce processus de transformation, s'ajoute la notion de « script » définie par Madeleine Akrich qu'elle utilise dans sa description des objets techniques comme l'ensemble des projections et des choix effectués par les concepteurs en fonction de présupposés techniques et sociaux qu'ils placent dans un objet :

> « Designers thus define actors with specific tastes, competences, motives, aspirations, political prejudices, and the rest, and the assume that morality, technology, science and economy will evolve in particular ways. A large part of the work of innovators is that of "inscribing" this vision of (or prediction about) the world in the technical content of the new object. I will call the end product of this work a "script" or a "scenario". » (Akrich, 1992)

À ce stade, les objets techniques « blackboxed » incarnent cette vision des concepteurs et ne sont plus sujets au questionnement. Ainsi, un des objectifs de la thèse est de « unblackboxer » l'IMSI catcher notamment en reconstituant le dispositif et ses « scripts » par une démarche de recherche-création.

Le mode d'action de l'IMSI catcher et son fonctionnement sont aujourd'hui relativement connus des activistes, hackers et chercheurs et ceux-ci émettent de nombreuses critiques à son égard. On peut toutefois le rapprocher de la boîte noire telle que thématisée par les chercheurs en STS et Vinck pour deux raisons principales : d'une part parce l'usager du réseau téléphonique mobile ignore en tout ou partie l'existence de ce dispositif et de son fonctionnement et d'autre part à cause de l'apparente complexité de celui-ci. Ce phénomène fait écho à ce que le philosophe Gilbert Simondon souligne lorsqu'il s'intéresse au mode d'existence des objets techniques, le décalage entre « culture » humaine et nature exacte des techniques :

> « La plus forte cause d'aliénation dans le monde contemporain réside dans cette méconnaissance de la machine qui n'est pas une aliénation causée par la machine, mais par la non-connaissance de sa nature et de son essence, par son absence du monde des significations, et par son omission dans la table des valeurs et des concepts faisant partie de la culture » (Simondon, 1958, p.9-10).

Ainsi, les malentendus ou l'incompréhension liés à l'utilisation d'un dispositif ne sont pas causés le dispositif lui-même mais plutôt par une méconnaissance de l'utilisateur vis-à-vis du fonctionnement interne du dispositif, celle-ci peut être entre-autres due au processus d'invisibilisation et à l'opacité cités plus haut.

Par ailleurs, pour Simondon, afin étudier un objet technique il est nécessaire de s'intéresser d'une part à son « processus de concrétisation » et à sa relation avec son « milieu associé » d'autre part. Le processus de concrétisation est la manière dont il passe d'objet technique abstrait à objet technique concret, c'est-à-dire d'un objet composite à un objet « dont les éléments sont intégrés, fondus l'un dans l'autre dans une synergie de forme et de fonctions » (Deforge, 1985), notamment dans l'étude des éléments internes qui le composent de la manière dont ceux-ci sont assemblés[19]. C'est l'idée d'une « organicité » croissante[20], par laquelle chaque pièce « ne peut pas être autre qu'elle n'est » (Simondon, 1958,

19 Simondon prend pour exemple l'évolution du moteur thermique à combustion interne: « Ces ailettes de refroidissement, dans les premiers moteurs, sont comme ajoutées de l'extérieur au cylindre et à la culasse théoriques, géométriquement cylindriques ; elles ne remplissent qu'une seule fonction, celle du refroidissement. Dans les moteurs récents, ces ailettes jouent en plus un rôle mécanique, s'opposant comme des nervures à une déformation de la culasse sous la poussée des gaz » (Simondon, 1958, p.22). Ainsi la version ultérieure est plus « concrète » que la première.

20 Simondon compare l'évolution les objets techniques dans une analogie aux êtres vivants. Toutefois, pour lui les êtres vivants sont les seuls à être concrets dès les début, alors que les objets techniques ne le sont jamais de manière absolue.

p. 21). Mais l'étude seule de la « résonance interne » entre les éléments n'est pas suffisante, c'est pourquoi il propose aussi d'étudier le « milieu associé » de l'objet technique : c'est-à-dire ses conditions d'existence — plus particulièrement les conditions techniques, économiques et politiques. Toutefois, l'IMSI catcher est un objet difficilement observable dans ses modèles commerciaux, il est difficile de s'en procurer pour des questions de confidentialité et de coûts ; c'est pourquoi je propose d'adopter une position de concepteur-designer dans une démarche de recherche-création pour l'étudier que je développe au chapitre 3. Ainsi, si Simondon étudie les objets techniques par l'approche de leur milieu, les milieux associés l'IMSI catcher sont ceux des concepteurs, des surveillants et des techno-critiques. Si les derniers peuvent paraître relativement accessibles, les deux premiers le sont beaucoup moins, voire pas du tout pour des raisons de sécurité et de secret industriel. C'est pourquoi il semble pertinent de vouloir directement ouvrir la boîte noire afin de l'étudier, dans une approche similaire à celle que propose le Critical Engineering Group dans son manifesto :

> « 1. L'ingénieur critique considère notre dépendance à la technologie comme un défi autant qu'une menace. Plus la dépendance est grande plus il importe d'en analyser le fonctionnement interne indépendamment des droits de propriétés et dispositions légales. » (Oliver, Savičić, Vasiliev, 2011)

Je ne prends pas dans cette thèse une position d'ingénieur critique à proprement parler, mais j'adopte une démarche de recherche-création qui implique effectivement de devoir analyser l'objet en l'ouvrant (afin de comprendre son fonctionnement interne) et ce en contournant le secret industriel qui l'entoure et en restant attentif à certaines dispositions légales notamment liées au respect du droit à la vie privée et à l'utilisation du spectre hertzien.

1.5 Recherche-création

Pour traiter du cas spécifique de l'IMSI catcher qui reste relativement inexploré et afin de contourner son caractère confidentiel et le secret qui l'entoure, j'adopte dans cette thèse une approche de recherche-création exploratoire et expérimentale qui se situe dans un cadre théorique et méthodologique à l'intersection de pratiques de recherche en design, des études des sciences et des technologies et des *surveillance studies*. Ainsi, à partir de l'étude de textes juridiques et de catalogues de dispositifs publiés par des sociétés spécialisées dans la surveillance, je propose de concevoir et de développer une série d'expériences pratiques en design. Dans un premier temps, ces expériences s'attèlent à la reconstitution de différentes formes d'IMSI catchers, dans le but de mieux cerner leur fonctionnement, leurs limites et leurs faiblesses ; toutefois, la reconstitution de ces dispositifs comprend inévitablement une part de spéculation étant donné la

nature secrète des pratiques liées à cet objet. Dans un second temps, je m'attache à la conception et à la production de prototypes d'objets de contestation afin de questionner la légitimité de l'utilisation des IMSI catchers dans la surveillance. Enfin, la conception de scénarios à partir de méthodes de design prospectif et des usages possibles de ces dispositifs permettent d'envisager des futurs potentiels de l'objet IMSI catcher et des conséquences sociales de son déploiement. En révélant les relations habituellement invisibles entre les objets de la surveillance et les usagers, je tente à travers ma thèse d'évaluer le degré de concrétisation de tels dispositifs et de créer un débat plus large autour d'un objet confidentiel révélateur d'un régime de surveillance méconnu. Je fais aussi l'hypothèse de pouvoir amener une contribution épistémologique forte à partir de l'étude d'un objet technique opaque à l'aide de méthodes issues de la recherche en design, ainsi qu'une production de connaissances dans les champs disciplinaires de sciences sociales et des *surveillance studies* toujours à partir de cette recherche en design.

Les chapitres « Recherche par le design I : Refaire un IMSI catcher » et « Recherche par le design II : Vers des objets de contestation » ont chacun fait l'objet d'une publication, respectivement :

- Félicien Goguey. « Remaking an IMSI catcher » *continent. Issue 8.1-2/2019* : 176-185. <http://www.continentcontinent.cc/index.php/continent/article/view/339> consulté le 15.02.2022.
- Félicien Goguey. « Catch Me If You Can: Designing a Disobedient Object to Protest Against GSM Surveillance », *CHI EA '21 : Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, May 2021, Article No.: 32, 1–7. <https://doi.org/10.1145/3411763.3450363> consulté le 15.02.2022.

Ces articles ont été traduits, révisés et en partie réécrits afin d'être intégrés à la thèse.

Ce travail a également fait l'objet d'une publication plus large :

Nicolas Nova. & Félicien Goguey. Le black fax et ses dérivés, *Techniques & Culture 74*, "Techniques de lutte", 2020 : 150 -151. <https://www.cairn.info/revue-techniques-et-culture-2020-2-page-150.htm> consulté le 15.02.2022.

2
État de l’art

Comme nous avons pu le voir dans l'introduction l'IMSI catcher est un objet complexe dont l'analyse fait appel à différents concepts comme celui de la boîte noire et de l'attaque de l'homme du milieu. L'IMSI catcher est un dispositif technique parmi d'autres utilisé à des fins de surveillance et de contrôle. Aussi, pour l'étudier il est nécessaire de le considérer et de le situer dans un champ de recherche défini qui fait appel à la fois à une sociologie de la surveillance, à une sociologie des sciences et des techniques, mais aussi aux travaux de recherche en art et en design. C'est pourquoi je dresse dans ce chapitre un état de l'art depuis le panoptique à la surveillance téléphonique mobile en me référant à la fois à des travaux académiques, mais aussi à des travaux issus des milieux du *surveillance art*[21] et du design critique.

2.1 Du panoptique aux surveillance studies

Avant de s'intéresser directement à la surveillance du réseau téléphonique mobile, il convient de revenir rapidement sur la constitution des *surveillance studies* comme champ disciplinaire. Dans son ouvrage synthétique à propos des études surveillancielles, le chercheur en sciences de l'information et de la communication Olivier Aïm cite trois textes pionniers comme fondateurs de ce champ : *The Panopticon Writings* (Bentham, 1787), *The Principles of Scientific Management* (Taylor, 1911), *Économie et société* (Weber, 1921). Même si la surveillance n'est pas au cœur des travaux des auteurs cités, ceux-ci l'abordent à travers des problématiques plus larges, respectivement : la réforme de la prison, l'organisation du travail et la bureaucratie.

Ainsi, dans un des textes fondateurs de la théorie de la surveillance, *The Panopticon Writings*, le philosophe utilitariste Jeremy Bentham décrit un modèle d'architecture carcérale dans lequel le surveillant occupe une place centrale dans une tour et peut voir à tout moment les surveillés qui eux sont placés tout autour dans des unités individuelles, les surveillés eux ne peuvent voir le surveillant (Bentham, 1787). Ainsi les surveillés se savent potentiellement toujours sous surveillance, créant ainsi le sentiment d'être constamment surveillés. Toutefois, la notion de surveillance est quasi absente des écrits de Bentham, il emploie d'ailleurs le mot d'« inspection » qu'il considère comme un travail et une tâche à accomplir. Il faudra attendre que le philosophe Michel Foucault s'empare du modèle panoptique pour qu'il devienne un paradigme de la « société disciplinaire » et pour qu'il ait un réel impact dans les études de la surveillance.

21 Le *surveillance art* utilise les moyens technologiques habituellement utilisés à des fins de surveillance dans le but de commenter, de questionner ou d'offrir une réflexion à propos de celle-ci.

Frederick Taylor, qui a donné son nom à la théorie du développement industriel de masse, s'intéresse pour sa part à l'organisation du travail (Taylor, 1911). S'il n'est pas directement question de surveillance dans son ouvrage, Taylor propose une théorie du management qui présente l'organisation du travail de manière scientifique. Pour cela il émet un ensemble de « lois », de « principes » et de « systèmes » afin de répondre à « quatre opérations » principales :

> « 1. Développer pour chaque élément du travail de l'ouvrier, une science remplaçant les anciennes méthodes empiriques.
> 2. Spécialiser, former et entraîner l'ouvrier, au lieu de le laisser choisir son métier comme autrefois et apprendre comme il le pouvait.
> 3. Suivre de près chaque homme, pour s'assurer que le travail est bien fait suivant les principes posés.
> 4. Partager également la responsabilité et la tâche entre la direction et les ouvriers, la direction se chargeant de tout ce qui dépasse la compétence de ceux-ci. » (Taylor, 1911, p.53)

Ainsi, pour Aïm, l'ouvrage de Taylor constitue une « théorie de la surveillance au travail » indissociable « de la théorie du geste » qui repose sur « décomposition des mouvements, la spécialisation des gestes et la division des tâches des ouvriers » (Aïm, 2020, p.25), puisque l'ouvrier est placé sous constante observation ; ce regard sur l'ouvrier est l'objet d'une « division du travail appliquée à la surveillance » (Taylor, 1911, p.137). On retrouve notamment les théories de Taylor appliquées à la totalité de la vie des individus dans *Le Meilleur des Mondes*, le célèbre ouvrage d'anticipation dystopique d'Aldous Huxley (1931). Plus récemment, Gary T. Marx et Sharon Sherizen réexaminent le management scientifique de Taylor et la surveillance au travail à l'aune de l'apparition de nouveaux outils technologiques tels que l'identification biométrique et montrent comment ceux-ci viennent bouleverser les libertés individuelles des travailleurs et leur rapport à la hiérarchie (Marx et Sherizen, 1986).

Max Weber en analysant la société allemande du début du XXe siècle met en exergue l'émergence d'un modèle sociopolitique : le modèle « bureaucratique » qui repose notamment sur la notion d'autorité (Weber, 1921). Ainsi, Weber initie la notion d'idéal type d'une autorité parfaitement rationnelle incarnée par la bureaucratie. C'est par la bureaucratie que s'imposent la hiérarchie et les normes, c'est-à-dire une domination légale qui préfigure le caractère intrusif de l'administration contemporaine. Pour Oliver Aïm « l'ensemble des descriptions de Weber trouve une résonance très forte à l'heure où la surveillance est de plus en plus étroitement reliée à la question des données personnelles, des modalités juridiques toujours plus complexes de leur extraction et de leur livraison, mais aussi aux définitions de plus en plus difficiles à fixer entre "vie privée", "vie publique", "vie professionnelle", "vie intime", voire "vie secrète" » (Aïm, 2020, p.33). Ainsi, le travail de Weber préfigure les questions actuelles autour des données

(*data*) et de l'automatisation de leur traitement, notions particulièrement pertinentes dans la surveillance algorithmique que je développe plus loin.

Ainsi, en traitant indirectement de la surveillance les trois textes précédents constituent la toile de fond de la constitution d'un champ disciplinaire. Toutefois, lorsque l'on tient compte de la matérialité du dispositif sur lequel chacun de ces textes s'appuie, à savoir : la prison, l'usine ainsi que son architecture et ses registres de compte ; on réalise que les objets numériques (plus récents) échappent du cadre dépeint ici, en particulier l'IMSI catcher qui intervient en milieu urbain. Rappelons aussi, comme nous l'avons évoqué en introduction, que l'utilisation de l'IMSI catcher repose sur une opacité de fonctionnement. Or, cette opacité de fonctionnement est un élément accordant du pouvoir et un ascendant au surveillant sur le surveillé (Ziewitz, 2016) : dans ce contexte la notion de « méconnaissance de la machine » source d'« aliénation » (Simondon, 1958) induit un rapport asymétrique et apparait ainsi comme fondamentale dans les théories de la surveillance ; c'est pourquoi il conviendrait d'ajouter le texte de Simondon comme pionnier aux même titre que les trois précédents.

En outre, il convient de citer Michel Foucault comme précurseur des études surveillancielles contemporaines. Le modèle du panoptique architectural proposé par Bentham et cité plus haut est repris de manière plus abstraite en 1975 par Foucault dans *Surveiller et punir*. Foucault voit dans le panoptique un modèle théorique de contrôle social applicable à la société disciplinaire. Selon Gilles Deleuze « quand Foucault définit le Panoptisme, tantôt il le détermine concrètement comme un agencement optique ou lumineux qui caractérise la prison, tantôt il le détermine abstraitement comme une machine qui non seulement s'applique à une matière visible en général (atelier, caserne, école, hôpital autant que prison), mais aussi traverse en général toutes les fonctions énonçables. La formule abstraite du Panoptisme n'est plus « voir sans être vu », mais « imposer une conduite quelconque à une multiplicité humaine quelconque. » (Deleuze, 1986). Ainsi, pour Foucault la société disciplinaire s'exerce dans des environnements clos. Nous verrons plus tard que Deleuze propose à la relecture de Foucault un autre paradigme d'une surveillance plus fluide qui s'exerce partout à la fois basée sur la notion de « flux », c'est l'idée de la « société de contrôle » (Deleuze, 1990), pour lui « ce sont les sociétés de contrôle qui sont en train de remplacer les sociétés disciplinaires ». En outre, on peut voir la « société de contrôle » de Deleuze comme un prolongement de la « cage d'acier »[22] de Weber, rendu possible grâce au développement et à l'utilisation de technologies numériques dans le traitement des données. Ce paradigme annonce déjà un point de vue qui s'imposera dans les années 2000 et sur lequel je reviens plus loin : celui de la « surveillance liquide ».

22 La cage d'acier ou « iron cage » est un concept sociologique fondé par Weber qui se rapporte à la rationalisation de la vie sociale et qui agit comme un piège pour les individus opprimés par la bureaucratie.

Dans un même ordre d'idée, le sociologue américain James B. Rule formule la notion de « société de surveillance totale » dès 1973, soit deux ans avant la publication de *Surveiller et punir*. Dans P*rivate Lives and Public Surveillance : Social Control in the Computer Age* (Rule, 1973) il s'inspire largement de l'œuvre d'Orwell (Orwell, 1949) pour concevoir un modèle théorique :

> « Permettez-moi d'esquisser un modèle du développement le plus extrême possible de la surveillance de masse, un idéal type d'ordre social ressemblant à celui dépeint par Orwell, mais peut-être encore plus extrême. C'est ce que j'appelle une société de surveillance totale » (Rule, 1973).

Le travail de Rule examine le rôle des premiers systèmes administratifs informatisés tout en remettant dans un contexte historique certains des développements consécutifs ; par exemple, comment l'arrivée de l'automatisation et de la numérisation des données personnelles viennent perturber la notion de protection du droit à la vie privée ou « privacité » (*privacy* en anglais)(Ball et al., 2012). Néanmoins pour Rule, et comme le souligne Olivier Aïm, « il manque encore de nombreux facteurs pour que l'état de surveillance totale soit effectif : l'absence de limite dans la collecte de toutes les informations sur tout le monde ; l'extraction d'informations réellement pertinentes ; la centralisation complète ; l'immédiateté des flux d'information ; l'augmentation des « points de contact » avec les données qui ne soient pas limités aux infractions, aux informations administratives, légales ou judiciaires, par exemple » (Aïm, 2020, p.37). En outre, Rule présente des notions telles que le contrôle, la vie privée et la place des nouvelles technologies dans l'espace public, notamment urbain, qui occuperont une place centrale dans les études de la surveillance dès les années 2000. Plus tard et de la même manière, le travail de Gary T. Marx sur les agents de police travaillant sous couverture montre comment l'utilisation de technologies numériques telles que les caméras ou la numérisation des dossiers criminels ont permis l'émergence de nouvelles formes maintien de l'ordre (Marx, 1988).

D'autres chercheurs comme le sociologue Armand Mattelart s'intéressent à la globalisation de la surveillance (Mattelart, 2008). À travers un travail quasi archéologique, Mattelart retrace une généalogie de la surveillance moderne tout en s'intéressant aux concepts de sécurité et de contrôle qui régissent nos sociétés. Ainsi, il déploie un historique depuis les techniques de contrôle des individus, en passant par les systèmes de surveillance et de défense qui ont vu le jour dans le contexte de la Guerre Froide en prenant pour exemple les réseaux de surveillance planétaires comme Echelon et leur finalité militaire, jusqu'au Patriot Act et la nécessité d'informatiser et de « biométriser » la société pour garantir la sécurité nationale. Il montre largement comment les dispositifs technologiques sont mis au service du renseignement dans les démocraties face aux nouvelles menaces, notamment terroristes ; et comment les outils sont

mis à la disposition d'un ordre sécuritaire nous plaçant dans un monde proche de celui imaginé par Orwell dans 1984 (Orwell, 1949), tout en nous appelant à « une vigilance démocratique à l'égard des dispositifs d'intrusion ». La synthèse de Mattelart s'intéresse plutôt aux différents moyens technologiques et dispositifs qui permettent la surveillance pour en retracer l'histoire et ses concepts clés dans une dynamique de mondialisation.

Ce n'est qu'au début des années 2000 que les surveillances studies se constituent comme un champ disciplinaire à part entière, notamment à travers la création de la revue Surveillance & Society en 2002 (Castagnino, 2018). D'après les chercheurs en *surveillance studies* Kirstie Ball, Kevin Haggerty et David Lyon la contribution de leur champ est :

> « de mettre en avant, empiriquement, théoriquement, éthiquement la nature, l'impact et les effets d'un processus fondamental de structuration sociale. Ce processus englobe la collecte d'informations, habituellement (mais pas toujours) suivie de leur analyse et utilisation pour des buts de gouvernance sociale, environnementale, économique ou politique » (Ball et al., 2012, p.1, traduction de Castagnino, 2018)

Ainsi, plusieurs chercheurs tels que Gary T. Marx (1988, 2009, 2015), Stephen Graham (2010), David Lyon (1994, 2007), Helen Nissenbaum (2009, 2015) investissent ce champ et proposent d'autres modèles que le panoptique pour étudier la surveillance telle qu'on la connait aujourd'hui. C'est à partir de ces différents concepts et notions décrivant les enjeux de surveillance que je situerai le travail de recherche autour de mon objet d'étude. Comme nous allons le voir dans la partie suivante, j'utiliserai particulièrement les notions appliquées aux enjeux du numérique et des nouvelles formes de surveillance.

2.2 Surveillance algorithmique

Comme nous avons pu l'évoquer précédemment, le fonctionnement de l'IMSI catcher, comme tout outil numérique, repose sur l'exécution de code logiciel . Or, l'utilisation récente des technologies numériques à des fins de surveillance brouille la ligne de partage entre espaces privés et publics et fait émerger de nouveaux espaces de surveillance au sens large. Ces espaces reposent d'une part sur l'exploitation des propriétés physiques des ondes électromagnétiques ; d'autre part, ils reposent aussi et surtout sur l'utilisation de traitements automatisés des informations collectées.

Pour s'en rendre compte, prenons le cas du terminal d'aéroport abordé par les géographes Kitchin et Dodge (2011) ; pour eux ce sont les algorithmes et plus précisément le code logiciel qui constituent et produisent ce type d'espaces. Par

exemple, dans les aéroports la spatialité des zones d'enregistrement dépend du code logiciel : si celui-ci faillit, la zone passe d'un espace d'enregistrement des passagers à une salle d'attente plutôt chaotique. C'est ce qui mène Kitchin et Dodge à proposer la notion de *Code/space* comme étant les nouvelles expériences spatiales créées par l'utilisation du code logiciel dans une forme ontogénétique, ils donnent ainsi la définition suivante de *Code/space* :

> « un espace qui est dépendant du logiciel pour qu'il soit transduit comme prévu. Ici, la relation entre le logiciel et l'espace est dyadique ; ils sont constitués mutuellement, c'est-à-dire produits l'un à travers l'autre » (Dodge, Kitchin, 2011, p. 261).

Cette notion de *Code/Space* est à rapprocher de celle de « s*oftware-sorted geographies* » proposée par Stephen Graham : c'est à dire la façon dont le code logiciel va entraîner l'existence de situations de discrimination et potentiellement creuser les inégalités sociales et politiques, en particulier avec l'utilisation d'algorithmes de tri (Graham, 2005). Graham illustre les conséquences des « *software-sorted geographies* » en prenant l'exemple de la vidéosurveillance (de l'anglais *closed-circuit television* abrégé CCTV) et plus particulièrement l'utilisation d'algorithmes de reconnaissance faciale dans la surveillance vidéo ; pour lui cela permet d'établir une surveillance automatique et systémique dans lequel le visage devient un code-barre et où il est possible de désigner une population cible. Il souligne ainsi la façon dont la puissance de la surveillance vidéo est accrue avec le traitement des données collectées ; pour Graham, la prolifération de tels systèmes soulève de nombreuses questions politiques, sociales et éthiques cruciales.

En parallèle du regard analytique des chercheurs en sciences sociales, certains designers abordent ces thématiques d'une autre façon et s'emploient à déjouer les algorithmes de surveillance. C'est le cas de Adam Harvey, spécialiste de la vision artificielle, avec son projet *CV Dazzle* (2010-2014, fig. 2) qui propose un *lookbook*[23] de coiffures et de maquillages permettant de perturber la reconnaissance faciale. Les styles présentés jouent notamment sur la symétrie du visage, le teint de la peau, l'arête du nez et la couleur de la chevelure — régions faciales habituellement reconnues comme humaines par les algorithmes — afin de brouiller la reconnaissance et l'identification. Ce type de stratégies et de tactiques de contre-surveillance[24] sont notamment théorisées dans les *surveillance studies* à travers différents concepts sur lesquels nous reviendrons dans le chapitre 6.

Les notions de *Code/Space* et *software-sorted-geographies* sont pertinentes dans l'étude de la surveillance contemporaine, puisque celle-ci repose de plus en plus

23 Catalogue de photographies, notamment utilisé dans la mode, pour présenter une ligne de vêtements ou de styles.

24 Ensemble des mesures et techniques visant à empêcher la surveillance, inclut le plus souvent un ensemble d'actions (contre-mesures) qui permettent de réduire les risques de surveillance.

Fig.2. Adam Harvey. *CV Dazzle*. 2014. Capture vidéo.

sur des algorithmes de tri pour opérer ; que ce soit dans la vidéosurveillance, mais aussi sur Internet, avec par exemple l'utilisation de boîtes noires qui traquent les « comportements suspicieux » sur le réseau. Elles sont potentiellement pertinentes dans le cas de l'IMSI catcher pour tenter de le décrire d'une part et parce que celui-ci vient possiblement modifier le rapport entre algorithmes et espaces.

Si les travaux académiques abondent sur ce thème, d'autres artistes abordent aussi la question et s'attèlent à travers leurs travaux à décomposer et exposer cette surveillance algorithmique qu'elle soit étatique ou commerciale (surveillance conduite par les entreprises), comme c'est le cas dans *Face to Facebook* de Paolo Cirio (2011, fig.3 et 4). L'œuvre prend comme point de départ le vol d'un million de profils Facebook, parmi lesquels l'artiste en a retenu 250 000. Ceux-ci ont ensuite été réinjectés et rendus publics sur un site de rencontre en ligne fictif <lovely-faces.com>. À l'aide d'un algorithme d'apprentissage automatique utilisé à des fins d'analyse des expressions faciales, les faux profils sont mis en relation les uns avec les autres sur la base de leur « tempérament social » sur des critères tels que « suffisant », « facile à vivre » ou « sournois ». Ainsi, d'après le sociologue Jean-Paul Fourmentraux, dans l'analyse qu'il fait de Face to Facebook, « l'œuvre singe et parodie le pouvoir de Facebook et les dangers d'une véritable mainmise sur nos données, révélant l'insécurité de celles-ci et exposant littéralement les coulisses de leur exploitation technique via des logiciels de reconnaissance vocale, faciale et typographique. » (Fourmentraux, 2020, p.63). Cirio utilise ce détournement pour déclencher une prise de conscience sur l'utilisation des données privées mises en ligne et leurs conséquences politiques et sociales potentielles. En effet, cette performance a suscité des réactions de médias de masse, mais aussi des menaces de poursuite en justice ainsi que des menaces de mort. L'œuvre de Cirio préfigure en quelque sorte le scandale Cambridge Analytica (2014-2018), dans laquelle 87 millions de comptes Facebook ont été siphonnés pour ensuite être analysés et influencer le vote des électeurs dans les présidentielles américaines de 2017. Même si l'on peut aujourd'hui se poser la question de la capacité réelle et de l'influence qu'elle a eue sur le vote des électeurs (Hwang, 2020), cette manipulation à partir des données personnelles de millions d'utilisateurs est un exemple de « software-sorted geography », dans lequel le code logiciel joue un rôle prépondérant dans la constitution, la séparation et l'opposition de différents groupes.

On rencontre couramment ce type de configuration spatiale — ou géographique pour reprendre l'expression de Graham. Si l'on prend le cas d'Internet, comme le dit Dirk van Weelden, celui-ci « n'existe nulle part et opère simultanément dans le monde physique. Pour être plus précis : Internet produit un nouveau type d'espace-temps qui porte une relation vague et flexible avec le monde physique.

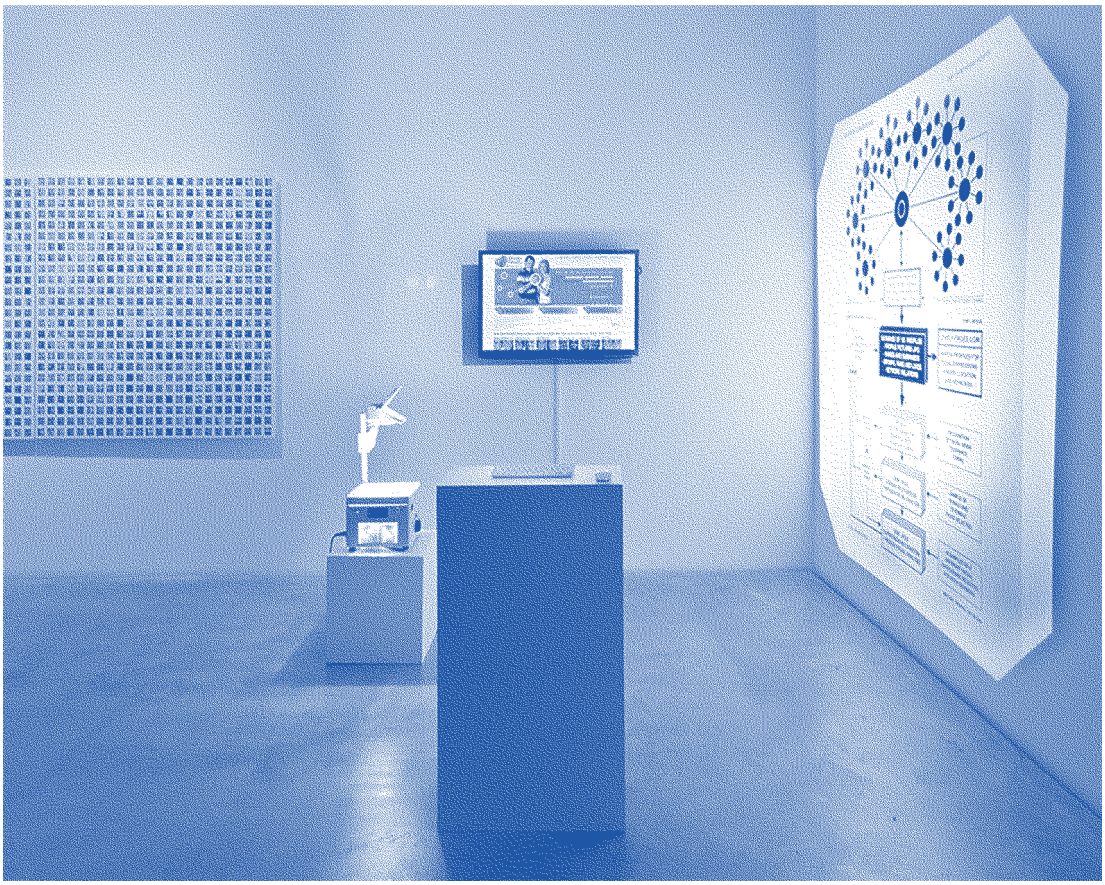


Fig.3. Paolo Cirio. *Face to Facebook*. 2011. Capture d'écran du site web <https://www.face-to-facebook.-net/>. / Fig.4. Paolo Cirio. *Face to Facebook*. Kellen Gallery of The New School, New York. 2014. Photographie de l'installation.

Le mot “espace” dans “cyberespace”[25] est très métaphorique et ne peut être séparé de l’activité menée dans celui-ci, puisque l’activité est ce qui produit cet “espace” » (Van Weelden dans Abrams et Hall, 2006, p.26). Les zones couvertes par le WiFi ou la téléphonie mobile rentrent dans cette catégorie d’espaces. Cette perméabilité est abordée par David Lyon dans la discussion qu’il a de l’idée d’une « surveillance liquide » avec Zygmunt Bauman en s’appuyant sur le concept de « modernité liquide »[26] avancé par ce dernier (Lyon, Baumann, 2013). Cet état dit « liquide » de la surveillance succèderait au modèle rigide du panoptique décrit par Foucault à partir de l’architecture carcérale inventée par Bentham, opposant ainsi le modèle solide et fixe à un modèle flexible et mobile. Les auteurs s’appuient sur les exemples des drones et des réseaux sociaux pour décrire ce modèle post-panoptique, mais il me semble que l’utilisation croissante des technologies sans fil et mobiles y participe aussi. En effet, dans le modèle de Foucault, le surveillant devait être présent à certains moments dans le panoptique, ce qui n’est plus le cas avec l’automatisation apportée par la surveillance algorithmique : si le surveillant est toujours le même, il peut maintenant se reposer sur le traitement automatisé des données pour déléguer sa tâche et intervenir sur un nombre beaucoup plus grand de surveillés. La surveillance liquide décrit ainsi des régimes de visibilité et d’invisibilité et se caractérise par des flux de données automatisés qui classifient constamment les individus. À mon sens, le régime d’invisibilité énoncé par Lyon est grandement favorisé par l’utilisation des technologies sans fil, autrement dit qui reposent sur l’utilisation de l’électromagnétisme, or l’action de l’IMSI catcher intervient principalement dans le spectre électromagnétique (ou espace hertzien).

2.3 Surveillance électromagnétique

Cet état liquide de la surveillance fait écho à la manière dont le philosophe Gilles Deleuze avait poursuivit la critique de Foucault, dans un texte fondamental (Deleuze, 1990). Ainsi, toujours dans une approche spatiale, il suggère à son tour que nous ne faisons que circuler d’un environnement clos à un autre, d’après lui « il n’y a pas besoin de science-fiction pour concevoir un mécanisme de contrôle qui donne à chaque instant la position d’un élément en milieu ouvert, animal dans une réserve, homme dans une entreprise (collier électronique) ». Aujourd’hui, le collier électronique décrit par Deleuze se matérialise pour la plupart d’entre nous

25 Cyberespace, néologisme façonné par Gibson à partir de « cybernétique » et « espace » dans sa nouvelle Burning Chrome (1982), utilisé depuis une trentaine d’années pour faire référence à l’espace créé par l’activité conduite au sein des réseaux numériques.

26 Le concept de modernité liquide est inventé par le sociologue et philosophe Zygmunt Bauman comme une métaphore pour décrire la condition de mobilité et de changement constants qu’il voit dans les relations, les identités et l’économie mondialisée dans la société moderne (Baumann, 1999).

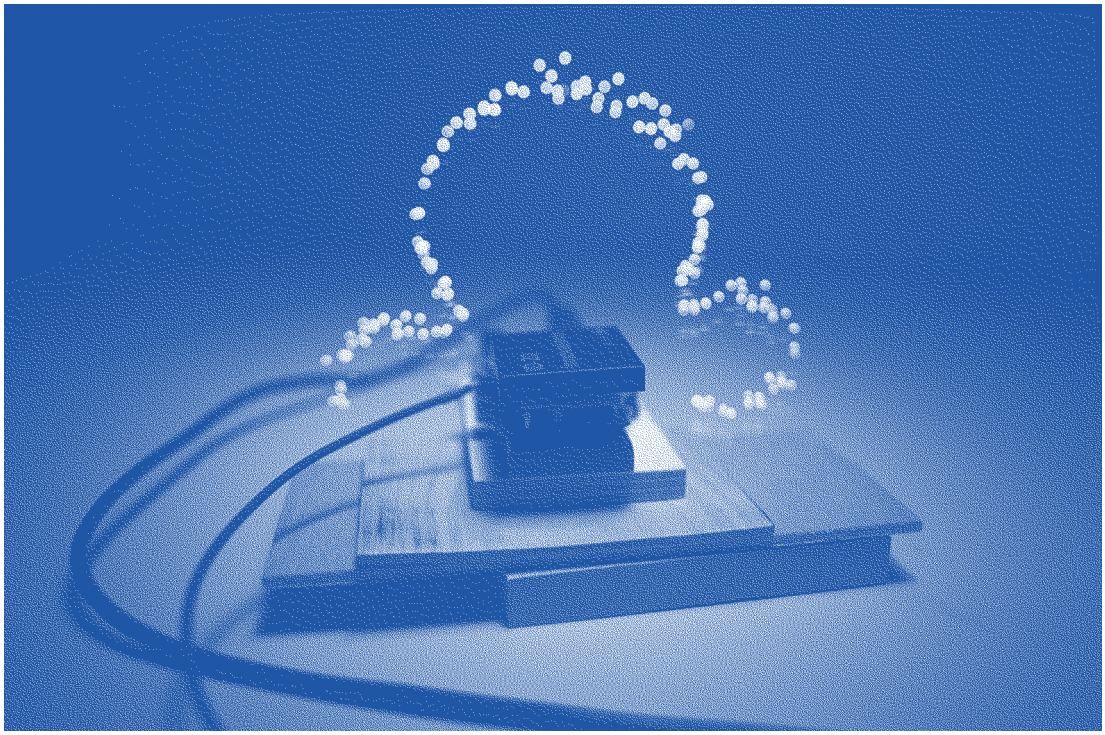
à travers le smartphone : un objet portable disposant d'interfaces radio (GSM, WiFi, Bluetooth…) identifiables par des adresses physiques uniques. Dès lors, les points d'accès WiFi et les cellules GSM que nous rencontrons dans nos déplacements sont autant d'environnements clos à travers lesquels nous transitons et dans lesquels nous sommes identifiables. Ces sphères spectrales et numériques qui se superposent aux espaces tangibles remodèlent la ligne de partage entre espaces privés et publics et mettent en place des mécanismes de filtrage qui segmentent ces espaces. Ainsi comme le souligne le sociologue Adrian Mackenzie : « les réseaux tels qu'Internet, mais aussi le réseau téléphonique, sont devenus de plus en plus denses et imbriqués dans nos espaces de vie. Les problèmes infrastructurels liés à la présence de câbles et de fils partout ont été grandement bien que partiellement résolus par la multiplication des fréquences d'ondes radio » (Mackenzie, 2010, p.63). Si, comme le dit Mackenzie, les problèmes infrastructurels ont été partiellement résolus grâce au « tout sans fil », le recourt toujours croissant au spectre hertzien entraîne d'autres problèmes dans son sillage : d'une part, il n'est plus possible de se rendre compte de la place que ces infrastructures dans nos espaces de vie puisqu'ils ne s'imposent pas visuellement comme c'est le cas pour les câbles ; d'autre part, en accroissant l'imperceptibilité des réseaux, le sans fil renforce la méconnaissance des mécanismes et protocoles qui interviennent sur nos données y transitant.

C'est aussi cette sphère spectrale et globale que Laura Poitras explore de manière quasi documentaire (Poitras, 2016) ; la réalisatrice, journaliste et artiste contactée par Edward Snowden au moment de ses révélations y invite différents auteurs à aborder la question de la surveillance globale et électromagnétique en s'intéressant à différents objets tels que *Echelon*, la *National Radio Quiet Zone*[27], des interceptions de signaux de drones, satellites et de radars, des documents du FBI censurés. Poitras questionne dans son ouvrage le rôle de la surveillance globale et électromagnétique à travers des fictions, des extraits de journal de bord et des entretiens ; elle propose des débuts de solutions pour vivre dans une société qui collecte des volumes extraordinaires de données sur les citoyens.

D'autres artistes et designers, à travers leurs travaux de recherche, s'emploient à aborder l'imperceptibilité de la sphère électromagnétique et par extension la surveillance de celle-ci. C'est le cas du chercheur en design d'interaction Timo Arnall dans le projet de recherche *The Immaterials*[28] (2004 - 2008, fig.5 et 6). Sans forcément aborder le thème de la surveillance, il s'emploie à rendre visible

27 La *United States National Radio Quiet Zone* est une vaste zone blanche entourant l'observatoire de Green Bank au sein de laquelle la radiodiffusion est fortement limitée par la loi pour faciliter la recherche scientifique et le renseignement militaire. <https://fr.wikipedia.org/wiki/United_States_National_Radio_Quiet_Zone> consulté le 15.02.2022

28 <https://www.elasticspace.com/2013/09/the-immaterials-project> consulté le 15.02.2022



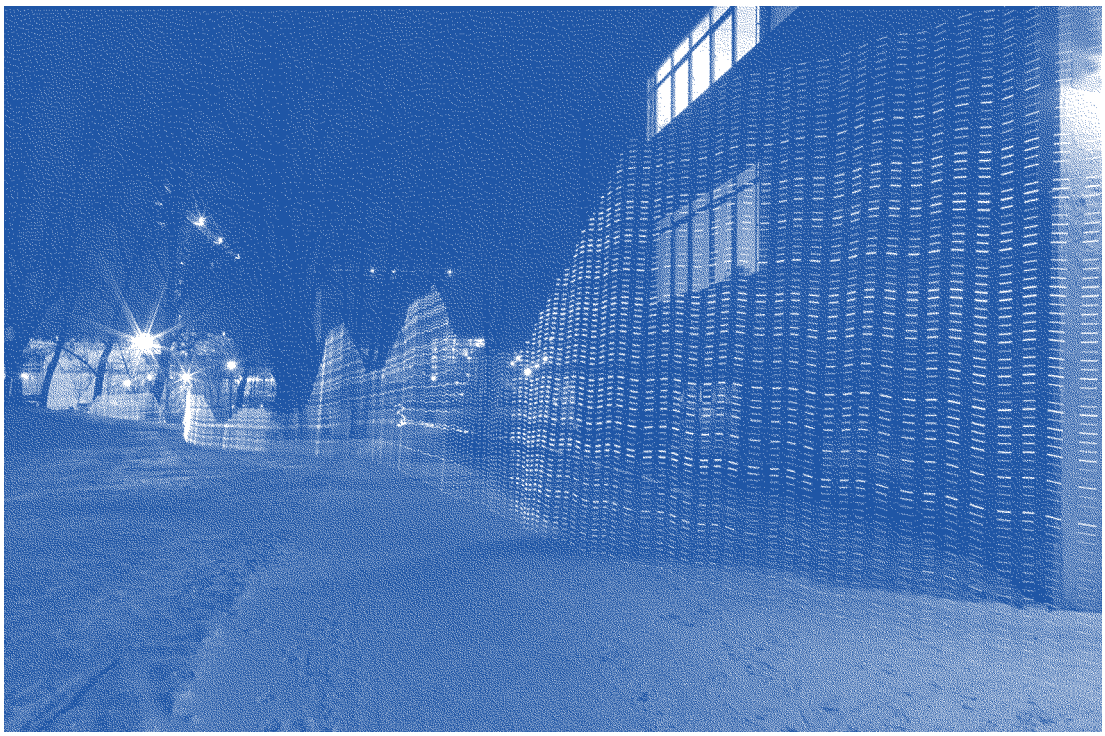


Fig.5 et 6. Timo Arnall. *Immaterials: Ghost in the Fields* et *Immaterials: Light painting WiFi*. 2009-2010. Photographies longue pose des dispositifs.

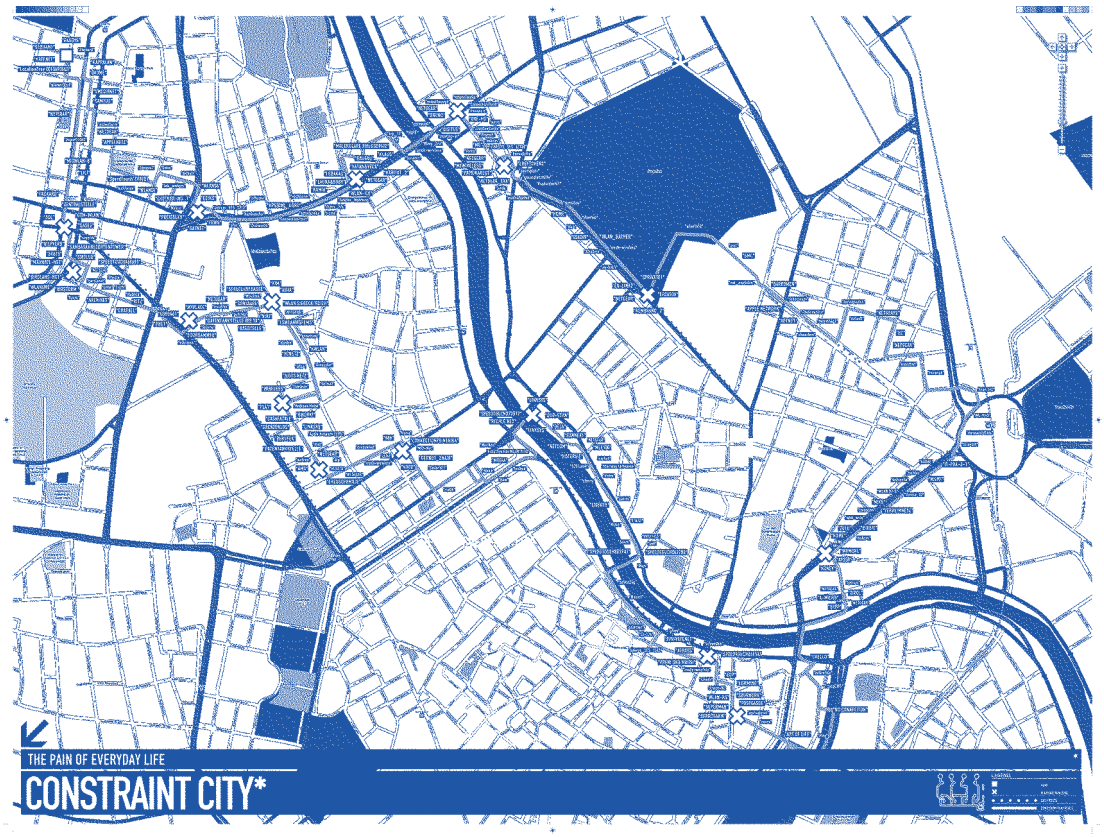


Fig.7. Gordan Savičić. *Constraint City, The pain of everyday life*. 2007. Photographie du dispositif. / Fig.8. Gordan Savičić. *Constraint City, The pain of everyday life*. 2007. Carte.

les technologies sans fil (WiFi ou RFID) à l'aide de dispositifs qui émettent de la lumière en fonction de la force du signal, il obtient avec une photographie longue exposition une image de la forme et de la portée des champs électromagnétiques générés par ces technologies. Les images obtenues révèlent une partie des bulles spectrales que nous traversons à tout moment et permettent de les visualiser afin d'en prendre la mesure : c'est un premier pas vers le dévoilement dans la surveillance qui y est conduite. C'est aussi le cas de l'artiste et ingénieur critique Gordan Savičić qui propose avec *Constraint City* (2007, fig. 7 et 8) une performance dans laquelle il se met en scène. Il porte un corset muni de puissants servo-moteurs reliés à une Nintendo DS WiFi. Cette dernière capte les signaux WiFi privés avoisinants et resserre immédiatement le corset sur son porteur en fonction de leur intensité. Cette performance reconfigure les déplacements quotidiens en une carte « schizogéographique » de douleur construite à l'aide de Google Maps. Gordan Savičić questionne dans cette pièce le rapport de l'individu à la ville et à la présence du spectre WiFi privé ; selon Adrian Mackenzie, il fait apparaître les conjonctions entre le corps du piéton même et les réseaux sans fil présents dans la ville de manière plus palpable. Si la douleur provoquée par le corset et les servo-moteurs n'est ressentie que par le porteur, les marques et contusions qu'ils provoquent sont visibles de tous. Basée sur une démarche quelque peu fétichiste et sadomasochiste, la pièce peut être vue comme une « expérience pragmatique de sentir des relations qui ne peuvent pas être facilement partagées » (Mackenzie, 2010, p.41).

D'autres chercheurs en design ont une approche plus spéculative, comme c'est le cas des designers critiques Anthony Dune & Fiona Raby. En 2007, ils proposent *EM Muzzle* (fig. 9), un dispositif fictif qui spécule sur l'avenir de la surveillance électromagnétique. Leur muselière électronique est un accessoire pour chien, qui se connecte à la partie du cerveau qui correspond à ses capacités olfactives. Une antenne reçoit et transmet les signaux électromagnétiques à cette zone hautement sensible. Dans le même temps, la muselière bloque la vue et l'ouïe du chien, afin que celui-ci puisse guider son maître dans une zone libre de toute surveillance électronique. Ce projet est destiné à être exposé et il est présenté sous la forme d'un objet en carbone non fonctionnel et d'un rendu 3D d'un chien portant le dispositif. S'il ne formalise pas directement la surveillance électromagnétique, cet objet permet de poser des questions par rapport à la légitimité de celle-ci et au respect de la vie privée dans un futur proche. Malgré le caractère décalé et spéculatif de ce travail qui parait peu crédible par rapport au fonctionnement même du dispositif, typique de l'approche de forcer le trait de Dunne et Raby, ce projet est intéressant parce qu'il entraîne un décalage avec la réalité de ce qu'est la surveillance.

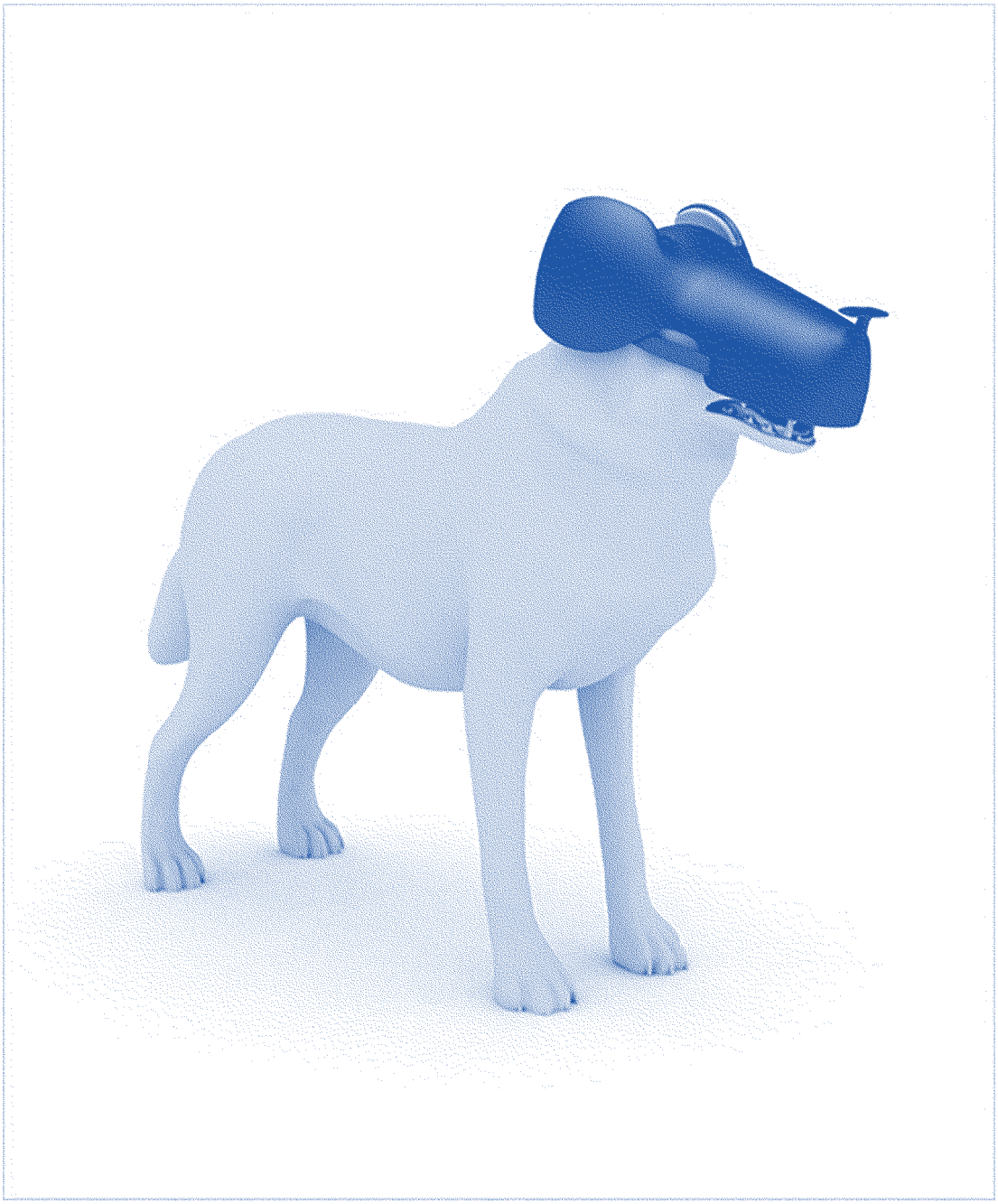


Fig. 9. Anthony Dunne, Fiona Raby. *EM Muzzle*. 2007. Modélisation 3D du dispositif.

La téléphonie mobile trouve sa place dans cette sphère électromagnétique, mais comme son nom l'indique elle a la particularité de permettre une mobilité constante (de cellule en cellule, ce qui n'est pas le cas du WiFi par exemple[29]), c'est pourquoi il est important de l'étudier dans sa singularité.

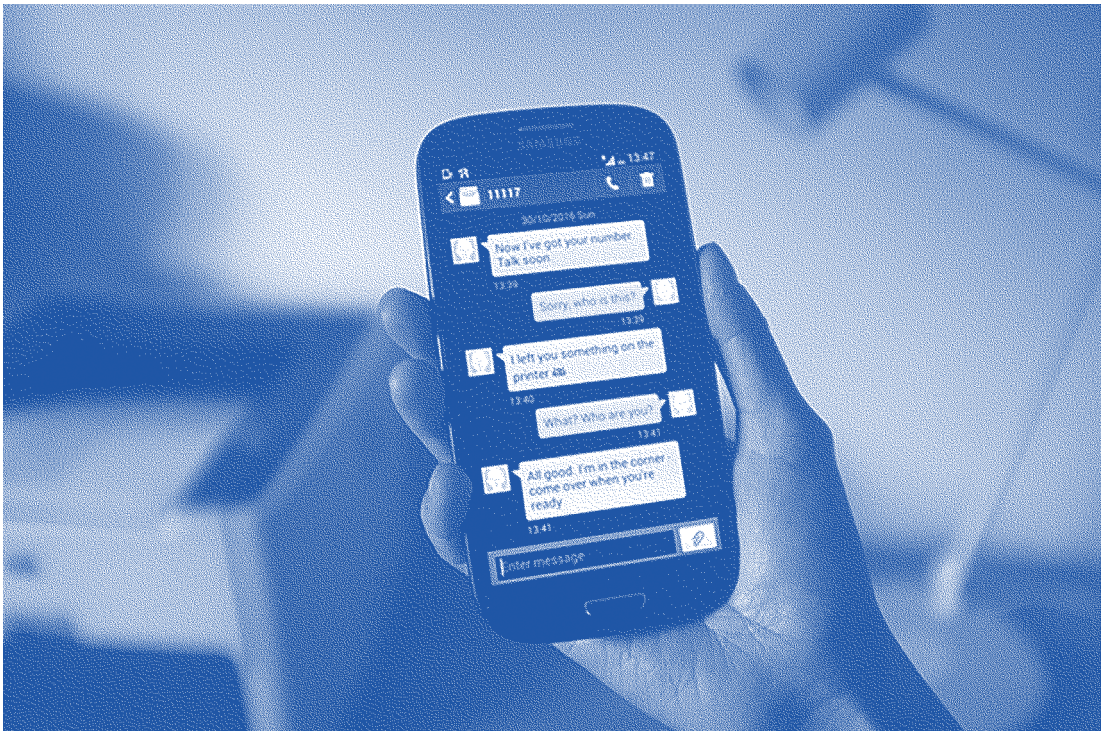
2.4 Surveillance téléphonique mobile

Comme nous avons pu le voir dans l'introduction, l'usage du réseau téléphonique mobile à des fins de surveillance par les acteurs gouvernementaux (douanes, police, services de renseignement), ainsi que commerciaux (entreprises dans des cas d'espionnage industriel), est documenté par des chercheurs comme Lisa Parks et Jason Farman, mais aussi par des artistes comme Julian Oliver.

Aussi, les technologies électromagnétiques sont aujourd'hui largement répandues et succèdent ainsi à l'architecture de murs et de fenêtres du panoptique dont les frontières nettes ont disparu. Ainsi, la chercheuse en sciences de l'information Helen Nissenbaum prend l'exemple de la téléphonie mobile qui intègre dans ses spécifications techniques l'obligation de pouvoir localiser l'emplacement d'un utilisateur du réseau dans un rayon de 50 à 300 mètres, afin de rendre possible une intervention rapide des secours en cas d'urgence (Nissenbaum, 2010. p.24). Comme elle le souligne cette capacité de localisation soulève des enjeux liés à la vie privée, notamment par rapport aux droits d'accès aux données ou à comment celles-ci sont stockées. Les questionnements autour de ces enjeux se retrouvent accentués avec l'intégration d'autres technologies aux appareils, comme le GPS, permettant une localisation encore plus précise, mais aussi par la capacité toujours croissante de stockage, d'analyse et de tri des données acquises. L'utilisation — entre autres — des technologies sans fil et mobiles rend donc possible l'apparition d'un modèle de surveillance fluide, plus ou moins imperceptible pour le surveillé, qui ne nécessite plus forcément de surveillant et qui ne structure plus l'espace comme les modèles précédents. En ce sens la téléphonie mobile, qui repose principalement sur l'exploitation des technologies sans fil — et qui dépend donc des ondes radiophoniques — participe au régime d'invisibilité qui favorise une forme liquide de la surveillance.

Dans ce contexte, l'utilisation grandissante des IMSI catchers comme nouvel outil de surveillance du réseau téléphonique mobile amène de nouvelles interrogations dans le domaine de la surveillance, notamment par ses aspects volatils et mobiles. D'après Lisa Parks, si un nombre important de thèmes ont déjà été discutés dans la recherche autour des questions de surveillance, l'IMSI catcher

29 C'est-à-dire en passant d'antenne relais en antenne relais de manière tout à fait fluide et imperceptible pour l'utilisateur, là où le WiFi requiert une action et un mot de passe pour s'y connecter la première fois.



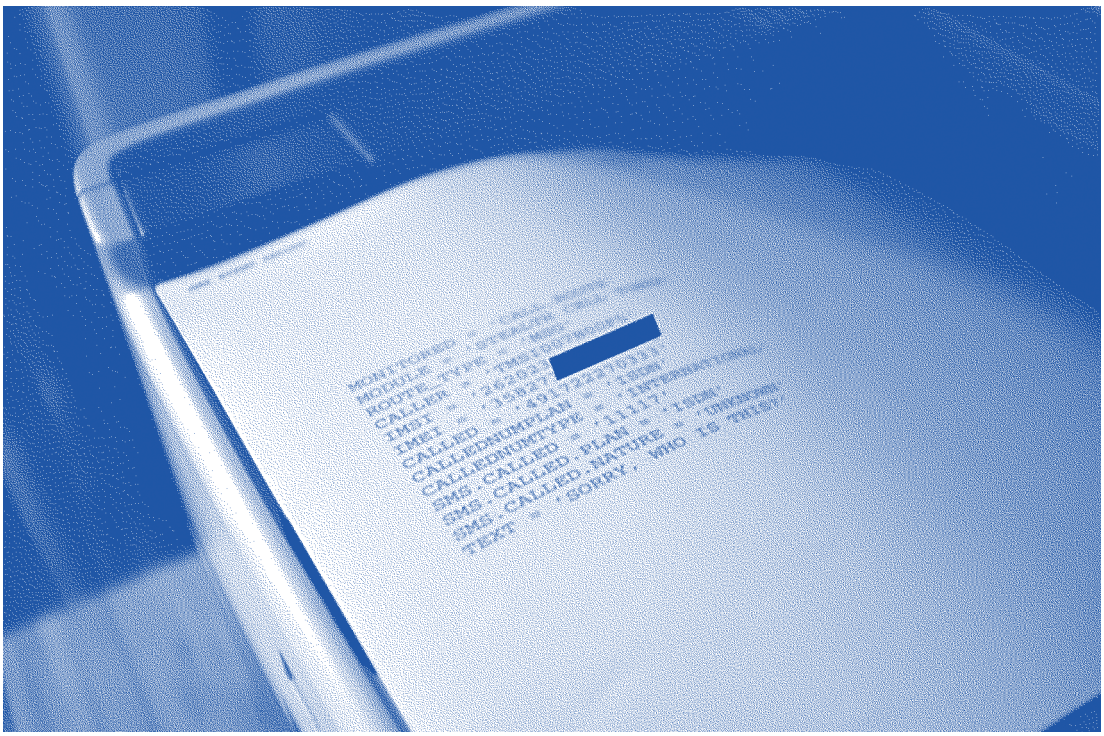


Fig. 10 et 11. Julian Oliver. *Stealth Cell Tower*. 2016. Photographies du dispositif.

reste peu étudié et constitue une préoccupation importante dans ce domaine notamment par rapport à ses usages et les controverses qu'ils soulèvent (Parks, 2016). En effet, ce dispositif qui tient dans une valise permet l'interception de l'identité des téléphones et des communications dans une zone donnée en se faisant passer pour une antenne relais. En employant le principe de l'attaque dite de l'homme du milieu, les IMSI catchers permettent la collecte d'informations personnelles, voire l'envoi simultané de messages textuels à l'ensemble des utilisateurs à sa portée. Ainsi, l'IMSI catcher rentre dans le rapport à la surveillance et aux sociétés disciplinaires, théorisé par Michel Foucault à travers la forme architecturale du panoptique, permettant au surveillant de surveiller sans être vu ni même devoir toujours être présent. Mais il le dépasse dans le sens où il rejoint d'une part la société de contrôle de Deleuze puisqu'il ne nécessite pas de bâti au sens architectural ; et d'autre part, la définition de la surveillance liquide discutée par Lyon et Baumann dans son invisibilité constante ainsi que dans le fait qu'il est très peu probable de savoir par qui (quelle instance gouvernementale ou commerciale par exemple) et quand il est utilisé.

Ainsi, l'artiste et ingénieur critique Julian Oliver illustre le fonctionnement de l'IMSI catcher et son caractère liquide dans une approche radicale et intrusive avec son projet *Stealth Cell Tower* (2016, fig. 10 et 11). Le dispositif est « une station GSM hostile qui prend la forme d'une imprimante inoffensive ». Lorsqu'un téléphone portable se situe à portée de la station GSM intégrée à l'imprimante, celle-ci envoie un message textuel, semblable à un message envoyé par un proche de l'utilisateur. Si ce dernier répond au message, le dispositif imprimera la réponse en plus d'un certain nombre d'informations liées au téléphone mobile. Cette installation imite un IMSI catcher, à travers l'impression des données liées au téléphone de l'utilisateur, le dispositif a deux objectifs : pour Oliver, dans un premier temps il pénètre la sphère privée de l'utilisateur à son insu et déclenche une prise de conscience ; dans un second temps il rend tangible la trace laissée par le passage de l'utilisateur dans l'espace surveillé. L'installation permet d'illustrer le caractère liquide de la surveillance algorithmique dans l'espace spectral : le dispositif peut-être déployé partout et n'importe quand (à la manière des IMSI catchers), on n'en connait pas les limites géographiques, et les personnes surveillées portent elles-mêmes une partie de l'infrastructure de surveillance (leur téléphone).

2.5 Surveillance studies et pratiques de recherche en art et en design

Parcourir l'histoire de la surveillance comme objet de recherche depuis Bentham jusqu'aux *surveillance studies* permet de situer en partie le champ disciplinaire dans lequel s'insère cette thèse. Toutefois, les *surveillance studies* laissent le cas précis et pratique de l'IMSI catcher relativement inexploré. En effet, c'est un objet inédit puisqu'il convoque à la fois les notions de liquidité, de mobilité, d'espace hertzien (Dunne, 1999) et d'automatisation du traitement des données, ainsi que des régimes d'(in)visibilité et de spatialité particuliers. Son investigation pourrait donc en partie renouveler les théories de la surveillance.

Comme les projets de designers et d'artistes décrits plus haut l'ont montré, nous avons vu au cours de ce chapitre qu'il était aussi possible de questionner l'utilisation de dispositifs de surveillance algorithmique, électromagnétique et/ou mobile à travers la conception et la production de dispositifs plastiques, numériques et interactifs. Suivant le cas, ces dispositifs ont pour but d'interpeller le public et visent souvent à déclencher une prise de conscience, voire parfois d'illustrer d'une manière artefactuelle des possibilités techniques, des enjeux, ou des controverses. À travers les différents exemples cités, on comprend que des travaux en art et en design, réalisés dans un contexte de recherche académique ou en-dehors, peuvent permettre d'aborder des questions de surveillance, notamment liées à des objets techniques. Cependant, on peut s'interroger sur l'écho produit par ces travaux auprès des visiteurs des expositions, par exemple dans leurs habitudes d'utilisation du réseau téléphonique. En effet, si le design critique ou le *surveillance art* ont souvent pour ambition d'éveiller l'esprit critique tout en s'inscrivant dans un cadre théorique, la question de l'impact de ce genre de production sur l'imaginaire ou les usages du public fait rarement partie intégrante du projet. On peut donc regretter que des études plus approfondies sur l'objet exposé ne soient pas menées et ne contribuent pas in fine à la production de connaissances.

De plus, ces travaux revêtent parfois une certaine technicité nécessaire à leur fonctionnement. En conséquence, ceux-ci peuvent se montrer cryptiques pour les non-initiés, ce qui parait paradoxal lorsque l'on veut apporter de la transparence à des systèmes de surveillance et communiquer autour de leurs problématiques. Pour pallier à cela, l'approche d'Arnall, développée dans sa thèse à propos de la technologie RFID et ancrée dans les recherches en design est pertinente (Arnall, 2014). Après avoir identifié le RFID comme phénomène technoculturel, en analysant un certain nombre de représentations et mythologies existant autour de cette technologie ; il s'en est servi comme matériau de design en menant une série d'expérimentations qui s'intéressaient à ses propriétés matérielles et immatérielles. Enfin, il a utilisé une troisième approche de « communication et

médiation du RFID » qui se focalisait sur les qualités culturelles, communicatives et « médiationnelles » de la technologie et sur la production de documents iconographiques et audiovisuels afin d'exposer les résultats de sa recherche en design à un public plus large. Arnall y voit un moyen pour la recherche en design de reconfigurer les imaginaires technoculturels en changeant la perception que l'on a de certains objets technologiques à l'aide de nouvelles interfaces et de nouveaux dispositifs. C'est en partie la démarche que je vais adopter en développant une recherche sur le design et l'histoire de l'IMSI catcher, puis en proposant une série d'expériences pratiques et enfin en utilisant des méthodes de design prospectif. Ainsi, cette thèse propose d'une part un apport méthodologique avec notamment un assemblage de méthodes courantes en design empruntées à la rétro-ingénierie employée en archéologie des médias, ainsi qu'aux techniques de reconstitution en histoire et au design fiction ; et d'autre part, une contribution dans un champ disciplinaire qui se situe à l'intersection des *surveillance studies* du design d'objet et du design d'interaction.

3
Cadre théorique et méthodologique

Ce chapitre présente le cadre théorique et méthodologique sur lequel je m'appuie pour développer la thèse. En effet, celle-ci se situe au sein de deux institutions : le programme doctoral Architecture et sciences de la ville (EDAR) à l'École Polytechnique Fédérale de Lausanne et le département design de la Haute École d'Art et de Design — Genève, au carrefour de la recherche en design, des STS et des *surveillance studies*. Il est donc nécessaire de revenir sur la recherche en design et comment elle s'est constituée, notamment pour des raisons institutionnelles en regard de l'académisation de celle-ci et de la production de connaissances établies à partir de pratiques d'artistes et de designers. On entend ici design au sens des arts appliqués[30] plutôt que des sciences de la conception : on le prendra dans l'acception de Nigel Cross qui le définit comme discipline (Cross, 1982) et étendue dans la définition que le chercheur en design Alain Findeli tente de lui donner :

> « Il est généralement accepté que la finalité ou le but du design est d'améliorer ou tout du moins de maintenir l'"habitabilité" du monde dans toutes ses dimensions : physique/matérielle, psychologique/cognitive/émotionnelle, spirituelle/culturelle/symbolique. » (Findeli, 2010, p.292)

La recherche en design se constitue comme discipline scientifique à partir de la seconde moitié du XXe siècle, notamment sous l'influence de Horst Rittel (Rittel, Webber, 1973) qui propose d'étudier la « science du design » qu'il enseignait à l'Université de Californie à Berkeley. Dès les années 1950, pour Rittel « toutes les procédures de design et toutes les formes des produits étaient interrogées et devaient être justifiées ou, à défaut, être rejetées comme arbitraires et inférieures » (Krippendorff, 2006, p. 310). Ainsi, la recherche en design vise la résolution de problèmes (*problem solving*) et se pose comme science de la conception. D'après Stéphane Vial : « c'est le début d'une vision du "design comme science" (design science), qui porte le rêve d'une science universelle de la conception incluant l'architecture et l'ingénierie et reposant sur une méthode logique et systématique du processus de conception » (Vial, 2015)

Cette velléité de cadrer la recherche en design remonte aux années 1960 et renvoie dans les pays anglophones à Bruce Archer (Royal College of Art), John Christopher Jones (The Open University), Christopher Alexander (Université de Californie à Berkeley) et Horst Rittel, elle s'est développée au cours des années suivantes dans le mouvement des *Design Methods*. Les *Design Methods* mettent fin à « la croyance dans l'idée romantique que le processus de design serait un processus créatif reposant essentiellement sur l'intuition solitaire d'un designer-artiste inspiré » (Vial, 2015). Cette assertion est un pôle possible, mais qui n'est pas forcément partagé par tous les chercheurs ; ainsi si les *Design Methods*

30 Les arts appliqués sont le secteur d'activité qui recouvre la conception des objets qui entourent l'individu : habitat, vêtements, communication…

préfigurent le *Design Thinking*[31], une autre manière de faire est celle venant des arts appliqués et il existe certaines controverses autour de la question.

Dans le contexte francophone, Lysianne Léchot-Hirt défend dans son article une vision de recherche-création (sur laquelle je reviens ci-après) qu'elle oppose à une « recherche en design scientiste » (Léchot-Hirt, 2015) et qui ne considèrerait comme académique qu'une recherche scientifique excluant une approche expérimentale. Pour elle, la recherche-création recouvre une réalité institutionnelle, dans laquelle cette thèse se situe — notamment dû à la nature du partenariat HEAD – Genève - EPFL. Léchot-Hirt affirme notamment qu'une « vision purement scientiste de la recherche en design est réductrice » et défend « une pluralisation des démarches de recherche en design » dans une démarche qui minimise les différences entre pratiques artistiques et pratiques de design tout en soulignant l'importance de la dimension expérimentale de la recherche-création qui prend sa source dans l'expérience, le vécu et le sensible et qui s'opposerait pour ses détracteurs à une certaine rigueur nécessaire à la recherche scientifique. Elle voit dans la recherche-création une proposition de se constituer de manière plus libre avec ses propres outils et langages et non-calqués sur ceux issus des sciences sociales ou autres champs de recherche constitués antérieurement. Enfin, la recherche-création par la production « [de] chaises, [d']affiches, [d']appareils, [d']interfaces numériques et [d']expositions, produit du raisonnement de design incarné dans des objets », ce que je défends aussi dans cette thèse à travers ma production de designer et de chercheur. Dans cette querelle idéologique, le chercheur en design Philippe Gauthier lui répond en développant son propos autour de la recherche-projet (que Léchot-Hirt qualifie de scientiste) en opposition à la recherche-création (Gauthier, 2015). Dans ce débat entre deux points de vue, Gauthier affirme que ces deux champs relèvent en réalité de deux pratiques distinctes et que s'il y a une « frontière à tracer entre deux camps, elle est donc bien entre la pratique de la recherche et la pratique du design (ou de la création) ». Il voit ainsi une irréductibilité entre ces deux pratiques et distingue le travail de chercheur de celui du designer ; il affirme d'ailleurs à ce sujet qu'« un chercheur en design peut être un bien mauvais designer ». Comme je le développe plus loin dans ce chapitre, ma démarche s'inscrit effectivement dans une vision plus proche de celle de Léchot-Hirt que celle de Philippe Gauthier ; d'une part, par les méthodes plurielles que je convoque, et d'autre part, par ma « sensibilité » de praticien et mon parcours en école d'art et de design. Pour autant, la méthodologie que je déploie ici, bien qu'expérimentale et en grande partie basée sur la pratique et la production de design, ne manque pas de rigueur épistémologique ni de réflexivité et apporte des preuves dans la recherche de la connaissance.

31 Le *Design Thinking* est une approche qui applique une méthode de résolution de problèmes (*problem-solving* en anglais) et puise dans les outils du designer afin de permettre l'innovation dans d'autres domaines que celui du design. Voir Tim Brown, Change by Design, 2009.

Quoiqu'il en soit, il y a des caractéristiques communes à ces deux pôles, par exemple tel que décrit dans le travail d'Alain Findeli, notamment autour de la notion de projet (Findeli, Bouscabi, 2005 ; Findeli, Costes, 2007). Ainsi, Findeli définit la recherche en design comme :

> « une quête systématique et l'acquisition de connaissances en lien avec l'écologie humaine généralisée considérée depuis une *designerly way of thinking*[32], c'est-à-dire dans une perspective orientée-projet » (Findeli, 2010, p.294).

Toutefois, sans rentrer dans les détails qui ne sont pas l'objectif direct de cette thèse, il s'agit de présenter en particulier les différents types de recherche en design auxquels je fais appel, à savoir : recherche sur le design et recherche par le design (Cross, 1982, Frayling, 1993).

Au-delà de la vision réductrice proposée par les *Design Methods*, Christopher Frayling défini dans *Research in Art and Design* trois axes pour la recherche académique en art et en design : « research on design », « research for design » et « research through design » (Frayling, 1993). Cette classification est aussi utilisée par Nigel Cross, en des termes légèrement différents, à savoir : « research into art and design » comme recherche historique, esthétique et « perceptuelle » ; « research through art and design » comme recherche à travers les matériaux et sur la base d'expériences pratiques, qui attache une importance particulière à la communication des résultats (Cross, 1982). Cross et Frayling posent donc les bases de ce qu'est la recherche en design, souvent qualifiée de recherche-création dans les milieux francophones. Cette thèse, dans l'étude d'un objet de surveillance du réseau téléphonique mobile reprend principalement deux de ces axes, à savoir la recherche sur le design et la recherche à travers le design. Néanmoins, les champs et formes du design ont largement évolué depuis et il est nécessaire d'actualiser cette vision.

Le chercheur en design Ralf Michel (2007) s'intéresse ainsi aux relations compliquées entre design et recherche en design, notamment comme forme de recherche pluridisciplinaire. Il invite plusieurs auteurs issus des milieux du design et de la recherche, mais aussi de l'ingénierie et de la cybernétique, à discuter la question de « faire du design » comme partie prenante de « faire de la recherche » à travers des essais, des études de cas et des exemples de projets de recherche récents. Ainsi, Michel et al. situent l'importance de la recherche en design en rapport au développement technologique, décrivent sa nécessité dans le développement des disciplines du design et soulignent son rôle fondamental dans les évolutions sociétales.

32 Autrement dit depuis un mode de pensée propre au designer.

Proche de la recherche à travers le design (Frayling) et sur la base d'une enquête auprès de designers et artistes, Lysianne Léchot-Hirt aborde la recherche-création[33] en design (2010). Elle s'intéresse aux méthodologies déployées dans ce champ à travers l'étude d'exemples de projets de recherche et propose un modèle qui souligne les spécificités de la recherche-création : la nécessité d'une certaine liberté et le besoin d'expérimenter, l'importance de l'interdisciplinarité et le fait de renouveler les modes d'évaluation des résultats de la recherche. Elle propose ainsi un modèle qu'elle nomme « *creasearch* » comme « modèle idéal typique » : « il se différencie des conceptions conventionnelles de la recherche scientifique en ce qu'il admet l'expérimentation créative comme expérimentation de recherche, et il se différencie d'une simple identification de la création à la recherche en restreignant le cadre dans lequel une activité de création peut prétendre comme activité de recherche » (Léchot-Hirt, 2010, p.77). En ce sens, le modèle proposé par Léchot-Hirt se dégage du cadre académique conventionnel trop contraignant et mal adapté pour les artistes et les designers et permet de replacer des pratiques en art et design comme pouvant produire de la connaissance dans « une culture de recherche singulière, mais compréhensible ».

Ces questions ont également été renouvelées au sein des différentes pratiques de design. Ainsi, le chercheur en design Ilpo Koskinen et ses collègues (Koskinen et al., 2011) s'intéressent à la recherche en design, mais cette fois-ci en prenant la perspective du design d'interaction et en replaçant l'utilisateur au centre de la démarche. Après avoir différencié le design, l'ingénierie et l'art comme disciplines indépendantes, les auteurs se posent la question du statut de la recherche en design dans différents contextes tels que celui du laboratoire (*laboratory*), du terrain (*field*) et de la restitution de la recherche (*showroom*). Ainsi, ils résument les conditions nécessaires à la recherche en laboratoire depuis la formulation d'hypothèses matérielles via la conception de prototypes à la nécessité de justifier un protocole expérimental ; de même, ils présentent des méthodes de terrain proches de certaines sciences sociales comme l'anthropologie et la psychologie expérimentale ; enfin, ils présentent la question de la valeur des connaissances produites et de leur restitution ainsi que la particularité du design quant à son utilisation comme outil de débat — « design for debate ». Ils soulignent également l'importance de l'hybridation des méthodologies dans une recherche en design notamment à travers des méthodes qui ne sont pas des instruments de recherche traditionnels tels que la conception et l'utilisation de modèles, de scénarios et de prototypes.

33 Le terme recherche-création apparaît dès les années 1980 au Québec et désigne toutes les démarches et approches de recherche favorisant la création, celles-ci étant propres à chaque projet: conception, expérimentation, production, saisie critique et théorique du processus créateur ; et dont le but est de produire divers types de connaissances.

Aussi, ma démarche — basée sur la pratique — se nourrit de différentes manières de faire : elle utilise principalement des méthodes de recherche par le design ; toutefois, une partie de recherche sur le design sert de préalable. Le terrain (*field*) de mon objet de recherche étant difficilement accessible, la méthodologie que je déploie se situe principalement dans le laboratoire (*laboratory*) et dans la restitution et la monstration (*showroom*), comme nous le verrons plus loin. Je présente donc le cadre théorique et méthodologique dans lequel s'insère la thèse en quatre parties : Recherche sur le design, Recherche par le design I : Reconstitution, Recherche par le design II : Prototypes, Recherche par le design III : Scénarios.

3.1 Recherche sur le design

La recherche sur le design trouve tout d'abord sa place dans l'histoire du design, notamment avec des travaux comme l'ouvrage de Kjetil Fallan (2010) dans lequel il retrace le développement de la discipline et explique comment il tire ses origines de l'histoire de l'art, du design industriel, de l'histoire culturelle et des études de la culture matérielle ; ou l'ouvrage d'anthologie d'Alexandra Midal (2013), recueil de textes en français portant sur le design en tant que concept, pratique et discipline parus entre 1841 et 2007 en Europe et aux États-Unis. Ces travaux de recherche sur le design peuvent parfois s'intéresser à un objet technique en particulier comme c'est le cas du travail de Quynh Delaunay dans *Histoire de la machine à laver* (1994). Dans le champ du numérique, la recherche sur le design aborde en général l'étude du processus de conception et de design. Elle peut avoir une perspective historique, comme le travail de Emanuele Quinz dans *Le Cercle de l'invisible* (Quinz, 2017) dans lequel il traite notamment de l'émergence du « paradigme de l'interactivité » ; sociologique si l'on prend pour exemple le travail de Dominique Cardon dans *Le design de la visibilité* dans lequel il s'intéresse au web 2.0 (Cardon, 2008) ; voire une combinaison de tout cela comme c'est le cas de *Joypad*, dans lequel les auteurs se penchent sur le design des manettes de jeux vidéo (Nova, Bolli, 2013). La recherche pour le design existe pour elle-même, afin de décrire les objets qu'elle étudie. Mais elle peut être réalisée également comme préalable à la conception de dispositifs techniques comme c'est généralement le cas dans les sciences de la conception.

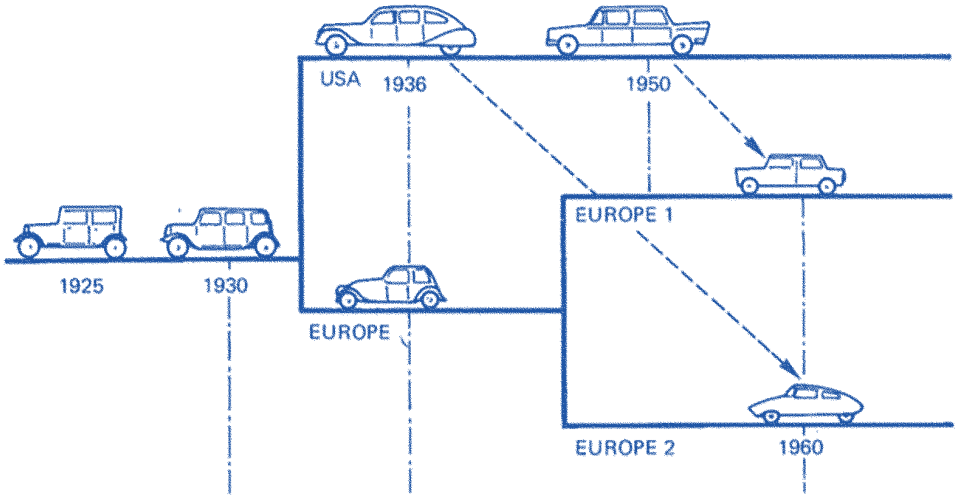
Toute démarche de recherche sur le design procède par enquête documentaire (historique, ethnographique) ou de terrain. Une enquête documentaire (l'approche choisie ici pour des raisons évoquées plus loin) repose sur la constitution d'un corpus de documents. Ainsi, cette partie de recherche sur le design s'intéresse à différentes implémentations existantes de l'IMSI catcher. Elle s'appuie sur un corpus de matériaux divers notamment constitué de catalogues de constructeurs de systèmes de surveillance ayant fait l'objet d'une fuite, d'objets présents sur des sites de vente en ligne (comme alibaba.com) qui proposent parfois une documen-

tation technique et d'observations de terrain (Revuelta, Milipol 2019). Sur la base du cadre théorique développé dans les travaux de Gilbert Simondon sur les objets techniques (Simondon, 1958), je fais l'hypothèse du caractère non « concret »[34] de l'IMSI catcher.

D'autre part, il s'agit ici d'identifier les différentes « lignées techniques » (fig. 12) de l'IMSI catcher, c'est-à-dire la diversité des occurrences ou implémentations de l'IMSI catcher (par exemple par la dissimulation de l'objet dans un vêtement ou dans un véhicule). Pour ce faire, je m'appuie sur la méthodologie développée par Yves Deforge qui repose sur les notions de principe, de fonction et d'évolution (de l'abstrait vers le concret, empruntée à Simondon) afin d'établir une typologie des différents modèles d'IMSI catcher passés et existants (Deforge, 1985). Les lignées techniques de Deforge sont également à rapprocher du travail en anthropologie des techniques d'André Leroi-Gourhan dans son ouvrage Milieu et techniques dans lequel opère une classification d'objets techniques et d'outils issus de la chasse, de l'agriculture, de la cuisine et de l'habitation selon certains critères tels que leur forme, leur fonction et leur mode opératoire (Leroi-Gourhan, 1945). Un autre exemple de classification d'un objet en lignées techniques est celui de la manette de jeu vidéo présenté par Nicolas Nova et Laurent Bolli dans *Joypad* (Bolli, Nova, 2013). En prenant comme point de départ la forme de base (une petite brique), ils établissent une généalogie de l'objet en intégrant les différents développements ergonomiques, des interfaces 3D et des boutons. Et cela en montrant que les différents choix de conception relèvent des enjeux liés tant aux actions de jeu, qu'à la morphologie des mains ou encore aux types de jeux disponibles. Ce faisant, cette reconstitution de lignées leur permet de saisir en quoi la manette de jeu vidéo est une interface qui permet d'analyser de multiples phénomènes socio-culturels liés à ce domaine, comme les présupposés des concepteurs à propos des contextes de jeu, de l'engagement du corps dans l'espace ainsi que des modalités d'actions réalisables dans les jeux.

Dans le cas présent, cette recherche sur le design est nécessaire comme préalable à la recherche par le design, notamment parce qu'il subsiste un flou autour du processus de conception et de design de l'objet étudié. En effet, le caractère confidentiel de l'IMSI catcher résulte en une rareté des informations sur la façon dont il est construit et dont il opère. Toutefois, certains documents accessibles de manière limités (catalogues de constructeurs qui ont fait l'objet d'une fuite par exemple) permettent de lever en partie le voile sur sa confidentialité. C'est pour cette raison que je me suis appuyé sur la constitution d'un corpus à partir de ressources diverses (brevets, catalogues, photographies), il est donc important d'établir une systématique pour définir les objets à sélectionner. Dans le

34 Car il n'est pas totalement intégré, mais relève plutôt de l'assemblage d'autres objets comme l'ordinateur, de cartes radio logicielle et d'antennes.



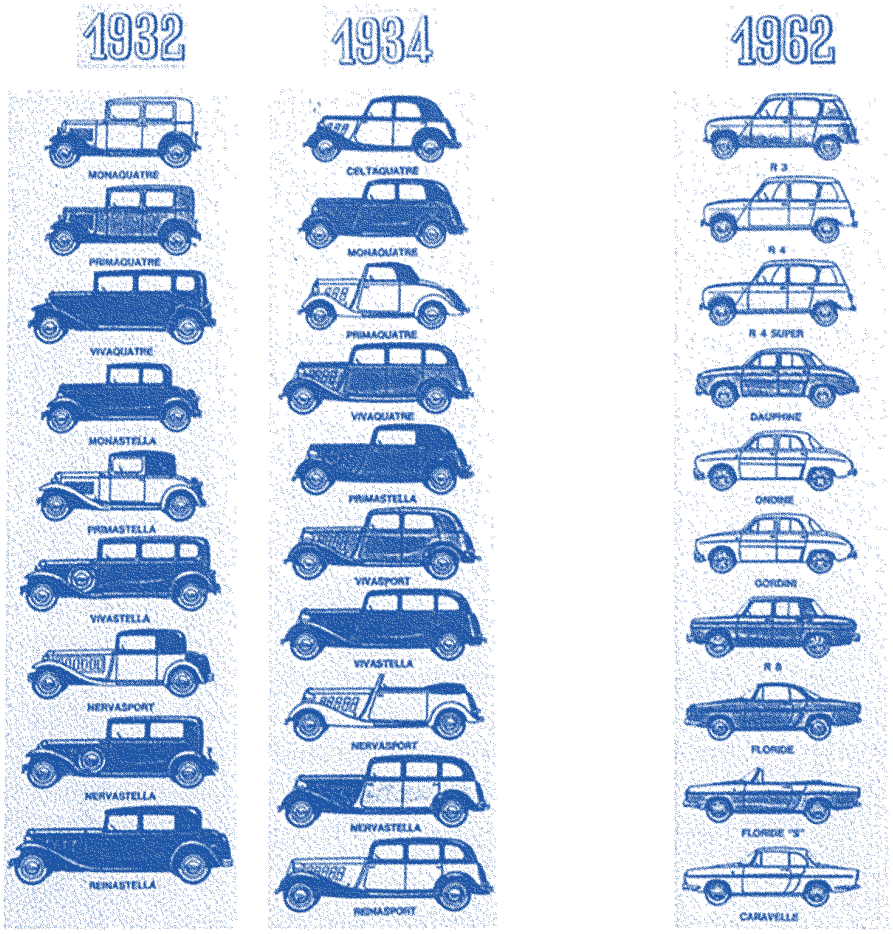


Fig.12. Yves Deforge. Exemple de lignées techniques dans *Technologie et génétique de l'objet industriel*. 1985. p.121

cas présent, la constitution du corpus de documents est délimitée d'une part en suivant la norme utilisée pour les télécommunications en l'occurrence le *Global System for Mobile Communications* (GSM), c'est-à-dire le standard utilisé pour les communications 2G ; et d'autre part par le mode d'action le type d'attaque opéré par l'IMSI catcher, c'est-à-dire l'attaque de « l'homme du milieu » ou « *man-in-the-middle* » qui consiste à intercepter une communication entre deux pairs sans qu'aucun des deux ne puisse en avoir connaissance.

L'analyse de ce corpus permettra également d'analyser le degré de concrétisation de l'IMSI catcher : d'une part par une analyse visuelle des éléments qui composent le plus souvent cet appareil (interface radio, antenne, ordinateur) ; d'autre part par les descriptions qui en sont faites dans les textes de loi et des manuels d'utilisation. L'identification de ces éléments, de leur rôle et de leur indépendance (que l'on peut toujours séparer en éléments distincts) permettra de s'assurer du caractère non concret de l'IMSI catcher. De plus l'analyse du corpus permettra l'identification de lignées techniques et d'établir une typologie des différents types d'IMSI catchers (embarqués, dissimulés, portables…) qui pourront éventuellement présenter un degré de concrétisation plus ou moins élevé. À partir de cette étude et de la dé-construction de l'objet IMSI catcher en éléments distincts et indépendants, il sera possible d'envisager une reconstitution de celui-ci à l'aide d'éléments disponibles au public ou « *off-the-shelf* » en anglais — c'est-à-dire commercialisés, c'est ce que nous verrons dans la partie suivante.

Par ailleurs, le cadre simondonien qui consiste à analyser les effets d'un objet technique sur son milieu associé est à rapprocher de ce que Stiegler appelle l'organologie (Stiegler, 2014). En effet, l'organologie générale étudie les relations entre organes physiologiques, organes techniques et organisations sociales. Ainsi, « l'organologie générale est une méthode d'analyse conjointe de l'histoire et du devenir des organes physiologiques, des organes artificiels et des organisations sociales. Davantage que cette perspective organologie, l'analyse du corpus sur l'IMSI catcher se rapproche de l'archéologie des médias (Parikka, 2012), une approche de recherche que le théoricien des médias Jussi Parikka définit comme « une analyse théorique raffinée des différentes couches historiques des médias dans leur singularité — un exercice conceptuel et pratique pour une cartographie précise des singularités esthétiques, culturelles et politiques des médias » (Hertz, Parikka, 2015). Cette approche est aussi celle adoptée par Emmanuel Guez au PAMAL (Preservation & Art — Media Archaeology Lab), notamment dans l'étude d'objets tels que le Minitel, ou de Erkki Huhtamo lorsqu'il analyse les « *moving panoramas* » (Huhtamo, 2013). Les praticiens de l'archéologie des médias sont aussi bien des universitaires que des artistes, des historiens que des théoriciens, des chercheurs que des bidouilleurs. Ils questionnent la matérialité des appareils qui nous permettent d'enregistrer, de communiquer et de traiter les données. Au contraire de l'historien qui déroule la généalogie des différents médias qui

se succèdent et leurs usages, l'archéologue des médias tente de creuser dans des couches plus profondes afin de faire émerger du nouveau dans l'ancien. En ce sens, l'approche que j'utilise dans le cas de l'IMSI catcher est similaire, puisque je m'intéresse à la matérialité du dispositif, à le démonter et à comprendre les effets qu'il a sur son environnement. Toutefois, l'approche développée dans la thèse se distingue de l'archéologie des médias puisqu'elle n'adopte pas un regard historique qui s'inscrit dans la durée, mais s'intéresse à un objet contemporain — puisque l'IMSI catcher est toujours développé et utilisé.

Enfin, étant donnée l'utilisation l'IMSI catcher dans les réseaux de communication, il serait tout à fait envisageable d'étudier l'IMSI catcher à l'aune de la théorie des médias, notamment au sens de Friedrich Kittler, pionnier de la *Medientheorie* allemande. En effet, ce champ de recherche s'intéresse à l'influence et aux enjeux à la fois esthétiques, épistémologiques, sociaux et politiques des « *Medien* » ; cette théorie réfute notamment qu'un médium puisse être un moyen de communication neutre et affirme qu'il a des implications beaucoup plus grandes que ce que l'on peut généralement percevoir. Ainsi Kittler s'intéresse à différents objets et montre des liens de parenté entre le gramophone et le développement de la psychanalyse, le cinéma, la guerre et l'armée, ou encore la machine à écrire et l'émancipation de la femme (Kittler 1986). Dans une approche similaire et dans le prolongement de ces recherches, s'inscrit le travail de Dietmar Kammerer qui lui s'intéresse aux aspects culturels de la surveillance en se penchant sur les représentations de celle-ci dans la littérature, le cinéma et la télévision par exemple (Kammerer, dans Ball et al., 2012), ce qui permet de s'intéresser à l'objet d'étude dans un système et à ses implications dans un cadre plus vaste qu'en le considérant comme indépendant. Il serait ainsi pertinent de s'intéresser à l'objet IMSI catcher comme le font Kittler et Kammerer à l'IMSI catcher vis à vis d'enjeux esthétiques, épistémologiques, sociaux, politiques et culturels. Toutefois, devant l'apparente complexité de l'objet cela semble difficilement réalisable, parce que l'IMSI catcher n'est pas un média en tant que tel et cela demanderait que l'on s'intéresse à la téléphonie mobile dans son ensemble délimitant ainsi une zone de recherche trop vaste qui pourrait faire l'objet d'un tout autre projet de recherche. Il apparait donc dans un premier temps nécessaire de l'isoler de son écosystème pour l'étudier en tant que tel, c'est à dire en tant que dispositif autonome (même si comme nous l'avons vu son fonctionnement est dépendant du réseau téléphonique mobile). C'est en partie pourquoi je propose une recherche par le design basée sur la reconstitution et dans une perspective ontologique afin de ré-ouvrir la boîte noire que je présente ci-dessous.

3.2 Research par le design I : Reconstitution

La première étape de cette recherche par le design s'attache à la reconstitution de plusieurs modèles d'IMSI catchers, à la fois au niveau matériel et logiciel. Cette reconstitution est basée sur les résultats de l'étape précédente « Recherche sur le design » et permet de mieux cerner l'objet dans ses limitations techniques, mais aussi formelles. Ainsi dans une approche qu'ils décrivent comme « *historical reconstruction* », les chercheurs en chimie et histoires des sciences Egen, Kvittingen, Lykknes et Wittje expliquent comment ils ont reconstitué, à partir de documents historiques et à travers une série d'expérimentations, un dispositif qui permet l'électrolyse de l'eau ; de la même manière, ils ont reconstitué une pile électrique en se basant sur la description historique de la pile de Volta de 1800 (Egen et al., 2012). À l'aide de cette approche de reconstitution historique, les expérimentations conduites et les objets produits permettent de couvrir deux aspects fondamentaux dans l'enseignement de l'électrochimie, à savoir la production de réactions chimiques à partir de l'électricité dans des cellules électrolytiques et la production d'électricité à partir de réactions chimiques dans des éléments galvaniques.

En prenant la perspective des humanités numériques, d'après le chercheur Jentery Sayers, le processus de reconstitution permet de poser des hypothèses sur les décisions prises dans le processus de conception, de comprendre les standards et normes implicites imposées dans la conception de l'objet ainsi que les présupposés sur les usages du dispositif et leurs évaluations (réussites, échecs) (Sayers, 2014). Ce processus permet d'explorer la présence de voies alternatives potentielles et pertinentes de l'évolution de l'IMSI catcher dans les étapes suivantes du projet. Cette méthodologie de reconstitution est à rapprocher de la rétro-ingénierie qui consiste à comprendre le fonctionnement d'un objet à travers son observation et en le démontant afin d'en analyser les composants. Sayers expose les raisons de prototyper le passé et déploie une méthodologie en prenant l'exemple d'un « bijou électro-mobile » parisien de 1867 (Sayers, 2015) ; à travers l'étude de schémas et d'objets d'époque et avec l'aide d'outils de prototypage rapide (machine-outil à commande numérique notamment) il reconstitue et teste différents mécanismes et hypothèses tout en les confrontant à la réalité de l'histoire culturelle de l'époque pour arriver à tirer des conclusions sur la manière dont cet objet a été conçu. Cette démarche n'est pas sans évoquer une certaine proximité avec l'archéologie des médias, notamment à travers l'utilisation de méthodes de rétro-ingénierie et qui se retrouverait dans des pratiques moins académiques mais qui relèverait plutôt du *hacking*.

En outre, dans une approche similaire du remake, l'artiste et designer Thomas Thwaites essaie de recréer dans une « tentative héroïque » un objet aussi simple qu'un grille-pain. Dans *The Toaster Project* (Thwaites, 2011), il décrit le processus

qu'il a mis en place depuis la collecte des matières premières nécessaires à la reproduction de l'objet jusqu'à leur transformation et leur assemblage. Dans un premier temps, Thwaites démonte le grille-pain dans le but d'étudier et d'analyser sa composition. Ainsi, il prend pour exemple un grille-pain « ordinaire » — c'est-à-dire que l'on peut trouver dans le commerce — et montre qu'il est composé de 404 parties indépendantes, puis les classe par matériaux utilisés (acier, mica, plastique, cuivre, nickel). Ensuite, dans sa tentative de reconstitution il essaie de réduire ce nombre au strict nécessaire en limitant au maximum le nombre de matériaux utilisés (métaux, plastique). En procédant par reconstruction d'un tel objet, Thomas Thwaites met ainsi en lumière les difficultés et les conditions technologiques, écologiques et leur interdépendance nécessaires à la conception et la production d'un objet en apparence simple et utilisé au quotidien.

Dans une logique similaire, Ratto et Boler (2014) présentent une série d'exemples qui abordent la culture DIY (le faire par soi-même) comme un moyen pour les citoyens d'ouvrir les boîtes noires des infrastructures technologiques dans une approche engagée et participative du *critical making*. Ces exemples issus du quotidien (carte d'identité, informations télévisées, presse, utilisation du *cloud*) illustrent en quoi cette approche active du faire qui s'oppose à une consommation passive permet aux citoyens qui endossent ainsi un rôle interventionniste, d'activiste, de *hacker*, de *modder* ou encore de bricoleur et permet la production de connaissances issues du faire par soi-même avec la technologie.

Garnet Hertz défend dans son approche du *Critical Making*, une position comparable pour laquelle il explique comment un travail de recherche qui passe par le « faire » — *making* — peut compléter et étendre une réflexion critique sur la technologie et la société (Hertz, 2012). Ainsi, dans la série de livres *Critical Making* éditée par Hertz, nous pouvons trouver des exemples tels qu'un *sextoy* DIY qui permet de réaliser des exercices de Kegel[35] en ayant un feedback lumineux ; ou *MaKey MaKey*, une carte électronique qui permet de réaliser des interactions entre objets physiques et objets virtuels et qui ne requiert aucune compétence en électronique ou programmation, mais qui demande à ce qu'on se pose la question du sens de son utilisation la plupart du temps en la transformant. Cette démarche permet notamment la production de réflexions critiques sur la façon dont sont produits nos objets du quotidien et une certaine réappropriation des technologies souvent considérées comme opaques par leurs utilisateurs.

En outre, Nicolas Nova et Anaïs Bloch, dans *Dr. Smartphone* (Nova, Bloch, 2021), étendent cette notion de *Critical Making* au *Critical Unmaking*, c'est-à-dire la connaissance acquise à partir du démontage « officieux » et documenté par les réparateurs eux-mêmes d'objets technologiques — en l'occurrence les smartphones

35 Exercices de renforcement du périnée.

démontés dans des ateliers de réparations. Cette approche du *critical unmaking* permet aux réparateurs de constituer une base de connaissances nécessaire à la réparation des téléphones qui va souvent à l'encontre de la volonté des constructeurs à ne pas rendre leurs téléphones réparables par le consommateur. On peut comparer cette discrétion souhaitée par les constructeurs de smartphones au caractère confidentiel de l'IMSI catcher. Dans ce sens, Nova et Bloch voient dans la notion du *critical unmaking* un rapprochement avec le « contre-faire » avancé par Laurence Allard, soit un scénario dans lequel le citoyen s'opposerait au contexte actuel et resterait « maître dans le cadre d'un scénario socio-technique sécurisé qui ne peut profiter qu'à l'intelligence collective environnementale » (Allard, 2015). Cette thèse, à travers le processus de reconstitution, vise à atteindre un objectif similaire en « contre-faisant » l'IMSI catcher.

En résumé, la démarche de reconstitution, qu'elle soit abordée d'une perspective historique, des humanités digitales, artistique, de design ou anthropologique permet de saisir les limites techniques mais aussi formelles de l'objet étudié, ainsi que d'identifier certains des choix effectués par ses concepteurs en fonction de normes et de standard implicites — soit les « scripts » de Akrich, mais permet également la production de connaissances historiques, conceptuelles, culturelles et techniques. Ces différents éléments qui permettent de mieux cerner l'objet d'étude nourrissent également la prochaine étape de recherche par le design.

3.3 Recherche par le design II : Prototypes spéculatifs

Cette partie de la recherche par le design consiste à concevoir des prototypes (fonctionnels ou non) qui interrogent l'utilisation de l'IMSI catcher. Ces artefacts présentent un savoir incarné dans une forme qui montre le mode d'action et/ou d'interaction d'un objet et un savoir situé dans un contexte donné. L'approche que je mets en pratique se situe à l'intersection de la rétro-ingénierie et du design spéculatif. En effet, cette seconde étape de recherche par le design bénéficie du travail de reconstitution effectué en amont afin de concevoir des dispositifs qui interrogent la légitimité de l'utilisation d'objets techniques à des fins de surveillance. En ce sens, la conception de prototypes est à rapprocher du design critique notamment dans le domaine des interactions homme-machine (HCI) ou de pratiques telles que l'ingénierie critique[36] (Oliver, Savicic, Vasiliev, 2011). Cet objectif s'inscrit dans la démarche de design spéculatif et design critique telle que décrite par Anthony Dunne et Fiona Raby, elle-même issue d'une pratique du design initiée dès les années 1960, notamment avec des pratiques comme celles de Joe Colombo qui prônait un *antidesign* (Midal, 2013), suivi par

36 <https://criticalengineering.org/fr> consulté le 15.02.2022

le *controdesign* dans les années 1970, ou le « design pour un monde réel » de Victor Papanek (1971).

Dans *Speculative Everything* (Dunne, Raby, 2013), les chercheurs et designers Anthony Dunne et Fiona Raby présentent des exemples issus de leur propre pratique et de leur enseignement mais aussi des champs de l'art, de l'architecture et du cinéma et montrent comment utiliser le design non seulement comme outil pour créer des objets mais aussi pour imaginer des futurs possibles. Ils définissent le design critique — opposé à ce qu'ils appellent le design affirmatif qui produit les objets du quotidien — comme un design qui emploie le design spéculatif et le design fiction et qui a pour but de questionner les suppositions et les conceptions à propos du rôle que joue les objets du quotidien (fig. 13). Plus largement le design critique a pour ambition de développer une réflexion à propos des types de futurs que les gens souhaitent ou ne souhaitent pas ainsi que d'ouvrir le débat et la discussion autour de futurs probables, plausibles, possibles et/ou préférables (fig. 14). À la différence du design critique qui se focalise sur les objets du quotidien, le design spéculatif se concentre sur la science et les applications et implications potentielles des technologies émergentes (Malpass, 2017). Ainsi, il extrapole des tendances socio-techniques et permet de se projeter dans un futur proche à l'aide d'outils tels que la construction de scénarios tout en s'appuyant sur la recherche technologique et scientifique. En ce sens, il sert à nourrir des alternatives à des assertions existantes en exposant les résultats d'une recherche à travers des objets matériels (Malpass, 2017). Dans les deux cas, que ce soit pour le design critique ou pour le design spéculatif, une des finalités est de débattre et de discuter de l'usage des objets du quotidien ou des technologies, c'est utiliser le « design pour débattre » (Dunne, 2008).

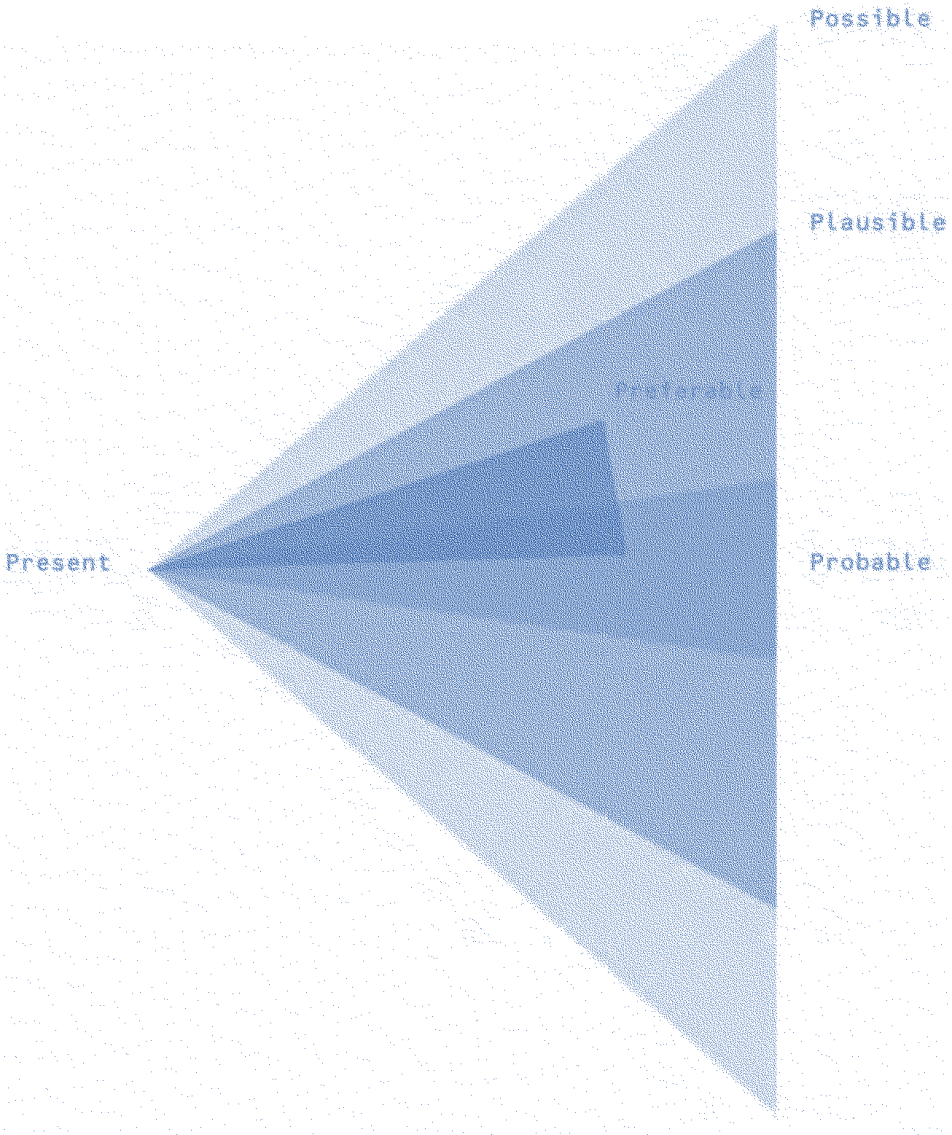
De la même façon le designer critique et chercheur James Auger, dans *Crafting the Speculation* (Auger, 2013) montre comment développer des présents alternatifs et futurs possibles d'une technologie (fig. 15). Pour lui, baser des visions possibles du futur sur des « trajectoires logiques » ou les « règles de la vie » permettent de « construire la spéculation en quelque chose de plus poignant, basé sur les interactions logiques d'une technologie émergente et taillé pour les exigences complexes et subtiles d'un public identifié ». Pour ce faire il s'appuie sur plusieurs exemples, dont certains issus des ses propres travaux comme le *Audio Tooth Implant* qu'il a réalisé avec Jimmy Loizeau (2001) : « un concept radicalement nouveau dans la communication interpersonnelle. Un dispositif récepteur sonore miniature et un récepteur sont implantés dans la dent pendant une chirurgie dentaire ordinaire. Ils offrent une forme de télépathie électronique puisque l'information sonore résonne directement dans la conscience »[37].

37 <http://www.auger-loizeau.com/projects/toothimplant> consulté le 15.02.2022

A	B
Affirmative	Critical
Problem solving	Problem finding
Provides answers	Asks questions
Design for production	Design for debate
Design as solution	Design as medium
In the service of industry	In the service of society
Fictional functions	Functional fictions
For how the world is	For how the world could be
Change the world to suit us	Change us to suit the world
Science fiction	Social fiction
Futures	Parallel worlds
The “real” real	The “unreal” real
Narratives of production	Narratives of consumption
Applications	Implications
Fun	Humor
Innovation	Provocation
Concept design	Conceptual design
Consumer	Citizen
Makes us buy	Makes us think
Ergonomics	Rhetoric
User-friendliness	Ethics
Process	Authorship

A/B, Dunne & Raby.

Fig. 13. Anthony Dunne, Fiona Raby. *Modèle A/B*. 2013.



PPPP. Illustration by Dunne & Raby.

Fig. 14. Anthony Dunne, Fiona Raby. Adaptation du cône des futurs de Voros. 2013.

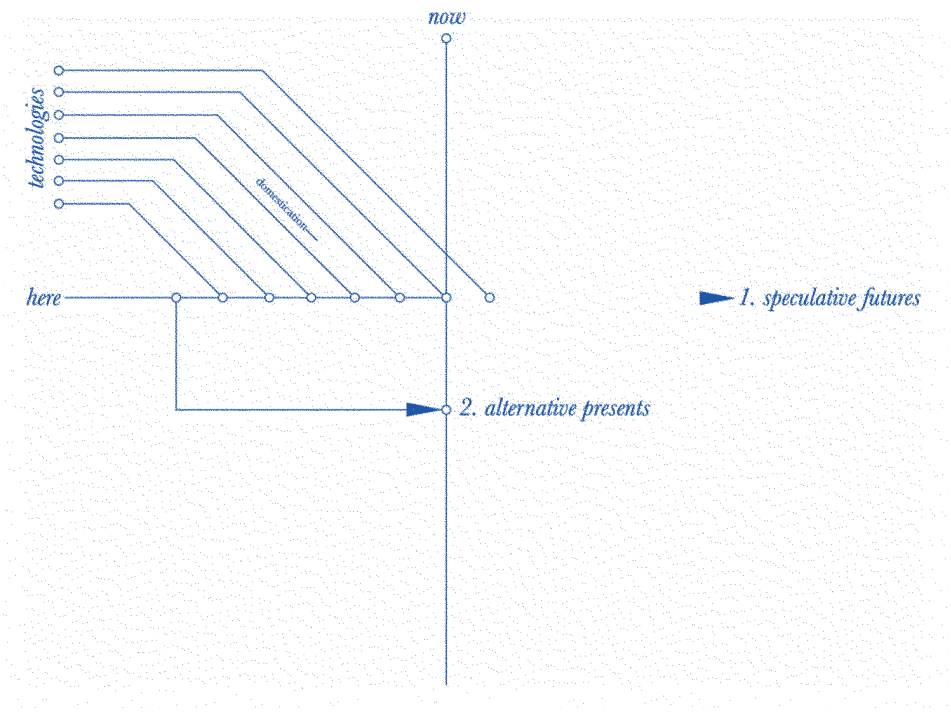


Fig.15. James Auger. *Alternative presents and speculative futures*. 2013.

L'historien du design Emanuele Quinz fait la critique du design critique en choisissant quatre épisodes de l'histoire du design : le design radical italien des années 1960, le design hollandais des années 1990, le *critical design* anglais des années 2000 et la scène contemporaine française (Dautrey, Quinz, 2014). Il identifie les stratégies du design conceptuel qui débouchent le plus souvent sur la production d'« objets étranges ». Il pose la question de l'efficacité d'un tel design, à savoir si « le recours à la fiction — dans lequel on n'utilise pas l'objet mais on en observe un usage étrange — [engage] le spectateur dans un véritable questionnement éthique ? » (Dautrey, Quinz, 2014, p.42). Il soulève également une possible perte de contact avec la réalité provoquée par le déplacement des « objets étranges » dans la fiction et évoque le risque qu'ils deviennent « de nouvelles incarnations du mythe », rendant ainsi la critique impuissante.

Ces possibles limites du design critique sont aussi exprimées par le chercheur en design Cameron Tonkinwise dans la critique qu'il fait du livre de Dunne et Raby (Tokinwise, 2014). Pour lui, les deux designers n'atteignent pas leur visée critique à travers leurs productions en partie parce qu'ils ne touchent pas le public ciblé. Il leur reproche notamment le côté statique de leurs objets, alors que ceux-ci devraient offrir une forme d'interaction physique afin d'en faire l'expérience sensorielle. De plus, Dunne et Raby n'offriraient pas assez de perspectives positives sur des types de futurs pour certaines parties du public. Il est rejoint en ce sens par Pedro Oliveira et Luiza Prado qui font une critique décoloniale du design spéculatif et critique qui d'après eux ne peut être réellement critique seulement s'il sort de sa zone de confort et commence à regarder au-delà des privilèges (Oliveira et Prado dans Fisher, Gamman, 2018).

Dans le cas de l'IMSI catcher, ce travail s'appuie d'une part sur la recherche préalable sur le design en se rapportant aux lignées techniques de Deforge mais en imaginant ce qu'elles pourraient être dans un futur proche ou un présent alternatif ; et d'autre part sur les différentes itérations issues de la partie reconstitution. En effet la recherche sur le design et la reconstitution constituent une base solide à partir de laquelle élaborer la spéculation. Pour cela, la littérature à ce sujet souligne l'importance d'appuyer ces trajectoires sur des faits réels et des tendances émergentes ou « signaux faibles » (Auger, 2013, Near Future Laboratory, 2021) afin d'ancrer ces objets spéculatifs dans des réalités vraisemblables. Ce qui permet ensuite d'apporter une réflexion socio -politico-technique sur le devenir de l'objet et ses trajectoires, reflétant ainsi sur ses usages présents.

Cette méthodologie a été en partie déployée lors du workshop *900 MHz : Protest*[38], durant lequel il était demandé aux étudiant.e.x.s de concevoir et produire des

38 Donné auprès des étudiants du Master Media Design de la HEAD — Genève, octobre 2019. Voir le chapitre 6 « Recherche par le design II : Vers des objets de contestation ».

prototypes permettant de protester contre la surveillance du réseau téléphonique mobile dans un cadre donné, celui de la manifestation. Ce workshop a donné lieu à une série d'objets *proof of concept* — qui permettent de montrer la faisabilité du procédé ou de l'innovation — et de propositions subversives qui permettent dans un premier temps de présenter un objet et son mode d'action et/ou d'interaction avec (1) les dispositifs de surveillance, (2) les manifestants et (3) les forces de l'ordre ; dans un second temps de tester des hypothèses formelles et des hypothèses d'interactions ; et, dans un dernier temps de déployer un espace discursif dans lequel on peut débattre de la légitimité de l'utilisation de tels dispositifs à des fins de surveillance et de maintien de l'ordre. C'est en partie ce que propose Anthony Dunne avec sa proposition de *design for debate* (2008), où il aborde l'exemple de la biotechnologie à travers la conception de prototypes spéculatifs pour soulever des questions éthiques dans la recherche dans ce domaine et son impact sur la société. Enfin, les artefacts issus de ce workshop ont été présentés dans une publication sous la forme d'un *fanzine*, qui devient ainsi un rendu pour les étudiants, en tant qu'objet intermédiaire (Vinck, 2009). C'est ce type d'objet intermédiaire entre une recherche sur le design et un prototype fonctionnel que l'on retrouve dans *Dr. Smartphone* (2021, Nova, Bloch), dans les bandes dessinées illustrées par Anaïs Bloch. Celles-ci, basées sur des observations de terrain constituent des formes de savoir qui comporte une valeur épistémique dans le sens où il permet de synthétiser des résultats en cours et d'être utilisé pour animer de premiers débats. Dans le cas présent, les prototypes présentés dans le fanzine se situent entre une recherche sur le design à partir d'observations de terrain (ici la manifestation) et des prototypes fonctionnels déployables sur le terrain tout en permettant déjà l'ouverture d'un espace discursif.

Dans ce sens, il serait aussi possible de dépasser le simple prototype qui fait office de preuve de concept[39] afin d'en faire un objet testé sur le terrain en conditions réelles, ce qui l'approcherait alors de la définition de Carl DiSalvo du *adversarial design* (DiSalvo, 2015). Ainsi, dans le cas d'un design testé, le prototype ne déploierait pas seulement un espace discursif pour questionner les relations entre théorie politique, design et technologie mais en ferait également un objet qui offrirait une nouvelle forme d'expression politique et un nouveau moyen d'action pour les citoyens. En ce sens, DiSalvo voit le *adversarial design* comme :

> « une tentative de fournir une réponse à la question "Qu'est-ce que cela signifie pour le design d'être politique ?" Le *adversarial design* est un design qui fait le travail de l'agonisme. Qu'est-ce que l'agonisme ? C'est une théorie politique qui souligne les aspects potentiellement positifs de certaines formes de conflit politique. Le *adversarial design* fait le travail de l'agonisme de plusieurs manières : il exprime des biais

39 En anglais *proof of concept*, ou démonstration de faisabilité, est une réalisation ayant pour vocation de montrer la faisabilité d'un procédé.

> et des positionnements conflictuels ; il offre des opportunités pour participer à la résolution de conflits de valeurs, de croyances et de désirs ; et il modélise des configurations socio-matérielle alternatives qui montrent des futurs possibles. » (DiSalvo dans Hertz, 2012)

On peut ainsi voir dans la proposition de DiSalvo une manière de pallier aux critiques faites au design spéculatif. Enfin, dans le cas de l'IMSI catcher, passer par la forme et l'ancrer dans le concret et la matière est une manière d'explorer le degré de concrétisation de l'objet. Toutefois, les objets produits dans cette thèse ne sont pas destinés à être testés en conditions réelles, et ce principalement pour des limitations techniques et légales.

L'intérêt de la démarche adoptée ici est de questionner à la fois les objets du quotidien, notamment avec des méthodes issues du design critique, mais aussi des technologies émergentes avec des méthodes provenant du design spéculatif. Les deux permettant de produire des futurs possibles et/ou des présents alternatifs afin de questionner l'IMSI catcher et les technologies sur lesquelles il repose. Ces méthodes sont très proches de celles utilisées dans la prospective et le design fiction que nous allons voir maintenant.

3.4 Recherche par le design III : Scénarios

Les prototypes conçus dans l'étape précédente permettent déjà le déploiement d'un espace discursif dans lequel il est possible de débattre. Toutefois, il est possible d'étendre cet espace discursif à l'aide de méthodes dites de *design fiction* et de construction de scénarios. Ainsi, cette partie s'attèle à la création de trois scénarios sur les futurs possibles de la surveillance du réseau téléphonique mobile ; ces scénarios ont pour but de faire apparaître des points de tension afin d'entamer une réflexion et susciter des débats autour de la légitimité et de l'éthique dans le déploiement de tels systèmes dans la société et dans leur place dans la ville. Cette approche critique et prospective du design, qualifiée de *design fiction* permet au designer de se libérer des contraintes techniques et technologiques qui rendent parfois impossible la démonstration, afin d'extrapoler des futurs possibles d'une technologie émergente. Ainsi, le terme *design fiction* est utilisé pour la première fois par Bruce Sterling en 2005 (Sterling, 2005, p.30) et par Julian Bleecker en 2009 (Bleecker, 2009). Sterling propose une définition formelle du terme comme « l'usage délibéré de prototypes diégétiques pour interrompre l'incrédulité face au changement »[40] (Sterling, 2013). Bleecker de son côté suppose que « les design fictions sont une manière oblique de voir les choses,

40 « Design Fiction is the deliberate use of diegetic prototypes to suspend disbelief about change » <https://www.wired.co.uk/article/patently-untrue> consulté le 15.02.2022

ou de renverser des logiques un peu trop standard en la matière » (Bleecker dans Nova, 2014, p.138). Ces définitions sont à rapprocher de celle de la prospective française comme étant l'ensemble de recherches concernant l'évolution future des sociétés et permettant de dégager des éléments de prévision ; ainsi considérée comme une science de « l'homme à venir » par son créateur Gaston Berger (Berger et al., 2007). Il existe dans le milieu académique anglophone une approche de recherche similaire notamment liée à l'utilisation de scénarios, telle que celle définie par Peter Schwartz et le scenario planning ou c'est-à-dire comment créer des scénarios sur la base de facteurs technologiques, économiques, culturels et politiques et les analyser à des fins de planification stratégique (Schwartz, 1991).

L'utilisation de scénarios prospectifs dans un travail de recherche-création consiste en l'élaboration d'une narration autour d'un objet ou des objets et permet par extension d'explorer les effets sur son ou leur environnement. Ces méthodes dites de *design fiction* permettent la création d'un discours incarné dans un monde fictif mais plausible (Near Future Laboratory, 2021). Ainsi, Mark Blythe conclut que le *design fiction* peut être utile pour (1) établir les espaces discursifs dans lesquels le travail prend place, (2) spécifier des concepts de design tout en maintenant un degré d'ambiguïté et (3) considérer des résultats possibles en créant des constatations fictives à partir d'études de terrain (Blythe, 2014). Dans le cas de l'IMSI catcher, la conception de scénarios prospectifs permet de s'affranchir de la technicité de l'objet (contraintes techniques) pour produire un discours qui s'étend au-delà de l'objet lui-même et qui est situé dans un contexte particulier. Ces scénarios produisent des trajectoires sur le devenir d'un objet, et rendent ainsi possible la critique des futurs possibles ou des présents alternatifs (Auger, 2013) à travers la production d'un discours ou d'un débat ; mais rendent aussi possible une réflexion sur son utilisation présente.

Tout l'intérêt du *design fiction* repose sur le choix de mise en forme et donc de construction des scénarios. Ainsi, l'agence de recherche Near Future Laboratory reprend dans *An Ikea Catalog from the Near Future* le célèbre catalogue du magasin de meubles suédois afin d'ouvrir une conversation sur le futur des objets connectés et de l'Internet des objets au sein de l'entreprise (Brown et al., 2016). Le catalogue, réalisé en partenariat avec l'industriel suédois, est ici utilisé comme un artefact de *design fiction* qui permet dans sa simplicité de présenter des scènes de la vie quotidienne convaincantes, tout en creusant les détails des objets représentés, en abordant des sujets connus et en en faisant émerger de moins communs. Ainsi, le catalogue compile une série d'objets et d'accessoires essentiels de la vie quotidienne qui dépeint un futur probable extrapolé de notre quotidien. Le but de ce catalogue est d'ouvrir une conversation auprès des consommateurs et des concepteurs sur le type de futur(s) que l'on souhaite, même si cela nécessite d'ouvrir des futurs que l'on craint. Ainsi, l'utilisation du *design fiction* dans une collaboration entre le milieu académique et l'industrie permet ici de mettre en

lumière les tensions à explorer dans le design d'objet en rapport avec les enjeux à venir. Le catalogue présente ici une portée critique, un état ambigu et un statut d'objet-frontière des designs proposés.

De la même façon, Paul Coulton, Joseph Lindley, Miriam Sturdee et Mike Stead (2017) prennent deux exemples pour décrire la « recherche en *design fiction*, accomplie à travers le *design fiction* ». Ils avancent que cette démarche relève dans les faits plutôt du « *world building* » que du *storytelling* ou de la construction d'une narration. Ils insistent notamment sur la diversité des formes employées pour créer des design fictions qui permettent de déployer des mondes fictionnels dans lesquels il est possible d'ouvrir des espaces de réflexion. Pour eux, la création d'une rhétorique dans un monde plutôt que dans une narration permet d'explorer ce monde fictif plutôt que de suivre une ligne narrative continue (Coulton, Burnett et Gradinar, 2016). Le *design fiction* s'apparente donc « à une carte d'un monde fictionnel qui peut être explorée de différentes façons, et la narration, si elle est utilisée, serait un chemin distinct à travers ce monde ».

L'utilisation de méthodes de construction de scénarios n'est pas le propre du *design fiction* et peut se retrouver dans d'autres disciplines. En outre, elles ont été utilisées dans le cadre du projet de recherche *Swiss Corona Citizen Science Project*[41] mené conjointement par l'EPFL, l'UNIL et l'IDIAP, dont le but était de comprendre les effets de la crise du coronavirus sur nos vies quotidiennes, développer des stratégies d'adaptation face à la crise et imaginer des futurs possibles après la crise, et ce en traitant différentes thématiques telles que l'habitat, la mobilité et l'économie locale. Ce projet a été mené à travers différentes étapes : un sondage national, la mise en place d'une application pour smartphone « Citizen Science », la conduite d'entretiens et enfin l'organisation de Citizen Think Tanks. Soucieux d'aborder un sujet en rapport avec ma thèse, j'ai développé le Citizen Think Tank 4 : Traçage des contacts et suivi numérique. Ce Citizen Think Tank proposait d'explorer et de discuter spécifiquement les enjeux, imaginaires et craintes soulevés par la question de la surveillance dans un contexte de crise sanitaire, notamment grâce à l'utilisation de scénarios. En effet, lors de l'épidémie de COVID-19, divers moyens numériques pour vérifier le respect des consignes sanitaires et endiguer la propagation du virus ont été considérés en Suisse, entre autres la mise en place d'applications de traçage des contacts ainsi que l'utilisation des données de téléphonie mobile. Dans le cas présent, l'utilisation de scénarios a permis de déterminer des futurs désirables, des futurs probables et des futurs non désirables depuis une perspective citoyenne ; en effet, l'analyse des discussions provoquées par la présentation des scénarios a permis de révéler ce que les citoyens étaient désireux de voir

41 <https://www.epfl.ch/labs/herus/index-html/projects/swiss-corona-citizen-science/> consulté le 15.02.2022

de la part du gouvernement dans la gestion la crise tout en développant une réflexion critique vis-à-vis des outils employés.

En conclusion, l'utilisation de méthodes de *design fiction*, notamment par le développement de scénarios et de mondes fictifs dans un futur plus ou moins proche mais toujours situé, dans un projet de recherche permet donc de produire des connaissances, qui se présentent sous la forme de trajectoires sur des futurs possibles et permettent une réflexion sur le présent. Dans le cas de l'IMSI catcher, l'objectif est d'explorer ses devenirs potentiels dans un futur proche, qu'ils soient souhaitables, préférables ou probables, et ce à partir de différents axes et facteurs socio-politico-techniques (apparition de la 5 G/disparition de la 2G, volonté politique de contrôle/volonté de transparence de la surveillance par exemple). De cette extrapolation seront produits trois scénarios qui permettront d'amener une réflexion sur les usages actuels de ce dispositif et plus largement des outils de surveillance basés sur les technologies numériques.

4
Recherche sur le design : Étude d’un objet confidentiel

L'IMSI catcher est un objet relativement confidentiel auquel il est difficile d'avoir accès, notamment parce qu'il est réservé aux forces de l'ordre et aux gouvernements ou à certaines grandes entreprises qui ont la possibilité de l'acquérir de manière officieuse (sur des sites de vente en ligne asiatiques notamment) et à cause de son prix élevé (qui peut atteindre plusieurs centaines de milliers de dollars). Afin de pouvoir l'étudier avec un point de vue de recherche-création, une première approche que j'utilise est la constitution et l'analyse d'un corpus de documents visuels et techniques (Rose, 2016); ceux-ci sont issus de différentes sources iconographiques, à savoir : de brevets, de sites de vente en ligne, de catalogues ayant fait l'objet d'une fuite, de photographies prises sur le terrain. Il s'agit donc ici de développer une recherche sur le design qui s'intéresse aux différentes implémentations existantes de l'IMSI catcher. Le caractère fragmentaire du corpus demande de rester attentif et de croiser les différents types de sources. Un des aspects abordés durant ce projet de recherche sur le design concerne le processus de concrétisation de l'IMSI catcher en tant qu'objet, c'est-à-dire le passage d'un assemblage de composants à un objet qui a une forme et une esthétique propre et qui est commercialisable en tant que tel, je m'appuie en partie pour cela sur les travaux de Gilbert Simondon sur les objets techniques (Simondon, 1958). En outre, ce dispositif fonctionne en exploitant des failles et des faiblesses du réseau téléphonique mobile et de ses protocoles, en ce sens il n'est pas un objet technique individualisé et autonome[42]. D'autre part, il s'agit ici d'identifier les potentielles « lignées techniques » de l'IMSI catcher, c'est à dire la généalogie des occurrences ou des implémentations de l'IMSI catcher (par exemple par la dissimulation de l'objet dans un vêtement ou dans un véhicule). Pour ce faire, je m'appuie sur la méthodologie développée par Yves Deforge (1985) qui repose sur les notions de principe, de fonction et d'évolution (de l'abstrait vers le concret, empruntée à Simondon, duquel il est ancien élève et dont il a poursuivi le travail en affinant la démarche) afin d'établir une typologie des différents modèles d'IMSI catcher.

Le corpus en question est constitué de :

- images extraites du *Government Cellphone Surveillance Catalogue* mis en ligne par The Intercept[43] en 2015 ;
- 5 captures d'écran du catalogue 2014 de Cobham Tactical Communications and Surveillance[44] ayant fait l'objet d'une fuite[45] ;
- 8 captures d'écran du site de vente en ligne Alibaba.com ;

42 Comme c'est le cas du moteur thermique à combustion interne présenté par Simondon.

43 <https://theintercept.com/surveillance-catalogue/> consulté le 15.02.2022

44 Maintenant *Domo Tactical Communications*, « une plateforme offrant des produits de sécurité et de surveillance sécurisés et fiables, en parallèle de systèmes de diffusion sans fil haute performance pour toute les industries ». <https://www.domotactical.com/> consulté le 15.02.2022

45 <https://theintercept.com/2016/09/01/leaked-catalogue-reveals-a-vast-array-of-military-spy-gear-offered-to-u-s-police/> consulté le 15.02.2022

- 5 photographies prises au salon Milipol 2019 par Marta Revuelta — une collègue designer et chercheuse qui travaille également sur des questions de surveillance[46] — où l'on voit des IMSI catchers ainsi que d'autres dispositifs de surveillance, de défense et de sécurisation ;
- 2 schémas extraits de brevets de dispositifs d'interception ;

soit un total de 30 documents toute nature confondue. Ces documents permettent d'établir un panorama qui donne à voir une partie du monde des distributeurs dans des objets finis et prêts à être commercialisés ; toutefois, en dehors de quelques spécifications techniques, ils renseignent peu (ou pas) sur le processus de conception de ces objets.

4.1 Vers une typologie ?

Dans les documents analysés se dessinent trois grandes catégories de dispositifs, ainsi on peut distinguer : les dispositifs portables (ou handheld devices) (pp.78-81), les dispositifs transportables (pp.82-87), les dispositifs embarqués (ou embedded devices, sur des véhicules aériens notamment tels que des drones) (pp.88-89). Cette typologie est principalement sur l'encombrement des objets, leur facilité à être transportés (autonomie, facilité de dissimulation) et leur mode d'action.

Dispositifs portables — *Handheld devices*

Les dispositifs portables — ou *handheld devices* — sont très proches par leurs formes de téléphones portables. En effet, ils ont la forme d'une petite brique qui tient dans la main et disposent d'un clavier alphanumérique et d'un écran.

L'antenne, la carte radio, la carte mère et l'alimentation (par batterie) sont directement intégrées au dispositif. Comme le décrit la documentation technique qui accompagne les images, ceux-ci sont souvent destinés à l'analyse passive des réseaux cellulaires et sont limités par leur capacité. En effet, ils ne peuvent écouter qu'une seule fréquence à la fois (*single band*), en d'autres termes une seule antenne relais, et sont souvent limités à des interactions passives avec celle-ci, c'est-à-dire limités à l'écoute de son activité (identité de l'antenne, puissance du signal, terminaux s'y associant, types de communications passées). De plus, ils n'ont que la capacité d'enregistrer les données capturées et de n'afficher que certaines d'entre-elles de manière très succincte. Afin d'exploiter celles-ci, il est le plus souvent nécessaire de connecter le dispositif à une base, ou à un ordinateur afin de les analyser après capture. Il n'est donc pas possible d'utiliser un dispositif

46 <https://revuelta.ch/> consulté le 15.02.2022

portable pour capturer et afficher des IMSI en temps réel. Néanmoins, un de leur plus gros avantage, lié à leur petite taille, est de pouvoir se dissimuler très facilement et de devenir tout à fait invisibles lorsqu'ils sont placés dans un vêtement ou un sac, ce qui permet des interceptions à courte portée en toute discrétion.

Dispositifs transportables

Les dispositifs transportables ont un volume plus conséquent mais permettent plus d'interactions avec le réseau. Ceux qui apparaissent sur les catalogues sont le plus souvent présentés sous la forme d'une grosse boîte noire qui contient une carte radio, un amplificateur et une alimentation, on voit parfois des antennes qui y sont directement branchées ou qui peuvent être déportées. Il est nécessaire d'y brancher un ordinateur (le plus souvent portable) pour pouvoir lui transmettre des instructions logicielles et le faire fonctionner, celui-ci apparait parfois dans les catalogues. Ils sont le plus souvent capables d'émettre et de recevoir sur plusieurs bandes de fréquences à la fois : les antennes choisies le sont en fonction des bandes de fréquences ciblées. On les voit le plus souvent installés à des points fixes ou transportés dans des valises afin d'être déployés rapidement, certains peuvent être embarqués ainsi dans le coffre d'une voiture ou d'un fourgon. Ils bénéficient aussi d'une plus grande portée (leur signal étant plus amplifié) mais sont plus difficiles à dissimuler que les dispositifs précédents, y compris sur des véhicules d'intervention où les antennes sont souvent à découvert (fig. 37 et 44).

Dispositifs embarqués — *Embedded devices*

Les dispositifs embarqués apparaissent dans les catalogues directement intégrés à des véhicules aériens (drone, avion ou hélicoptère) et il est difficile d'identifier les différents composants sur la base des photographies (souvent de mauvaise qualité ou miniatures). Toutefois, on peut deviner où est placée la charge utile sur la base des photos présentées : ils sont souvent intégrés à des capsules ou des conteneurs qui ont la forme de missiles : potentiellement pour des raisons aérodynamiques d'une part ; mais aussi pour des raisons techniques d'arrimage à l'appareil, comme le faisaient les forces aériennes britanniques durant la Seconde Guerre mondiale en transportant de la bière dans des réservoirs d'essence sur leurs bombardiers pour les parachuter à leurs troupes au sol. Le plus gros avantage de ces dispositifs embarqués est leur mobilité, qui leur permet de couvrir de vastes zones à l'échelle d'une ville ou d'une région. Leur utilisation a notamment été soupçonnée lors des manifestations Black Lives Matter de 2020, lorsque l'outil de visualisation Flightradar24 a permis de révéler le survol de celles-ci par des appareils effectuant des vols circulaires.

Lignées techniques pressenties

Deforge fournit trois outils méthodologiques de Deforge pour étudier la génétique de l'objet industriel et établir des lignées techniques (1985, pp.72-74) :

- la notion de « lignée génétique » que l'auteur définit comme « constituée par des objets ayant la même fonction d'usage et mettant en œuvre le même principe » ;
- la notion de « lois d'évolution », que l'auteur a empruntée à Simondon comme l'évolution de l'« objet abstrait » vers l'« objet concret »;
- « le réseau des relations réciproques que l'objet entretient avec les systèmes de production, de consommation, d'utilisation et avec ses congénères ».

Intéressons nous d'abord à la notion de lignée, pour déterminer celle-ci il est nécessaire de définir la fonction d'usage et ce que Deforge appelle le « principe ». La fonction d'usage revient à prendre la place de l'usager et de se poser la question « à quoi ça sert ? ». Aussi, Deforge définit la notion de principe « comme une "essence technologique" qui se manifeste par des solutions technologiques et des formes (mais pas toutes les solutions ni toutes les formes) qui le font se situer entre l'expression du problème et sa solution achevée » (Deforge, 1985, p.101). Pour Deforge, les objets qui ont la même fonction d'usage constituent une famille et les objets qui ont la même fonction d'usage et le même principe, classés dans un ordre chronologique constituent une lignée génétique.

Ainsi chacune des catégories d'IMSI catchers présentées ici (portables, transportables, embarqués) peuvent donner lieu à une ou plusieurs lignées techniques potentielles. En effet, les dispositifs ont la même fonction d'usage : « identifier des terminaux mobiles et intercepter des communications » et ils ont des principes qui diffèrent légèrement selon les modèles. Toutefois, il est difficile d'établir des lignées génétiques sur la base des documents étudiés. En effet, il n'est pas possible d'établir une chronologie claire des dispositifs présentés et de savoir lequel découle de l'autre. Aussi, si en recoupant les différentes informations il est possible d'établir le « principe » de chacun, il n'est pas possible de déterminer lequel vient avant l'autre. C'est pourquoi, dans le cas de l'IMSI catcher, il est plus prudent de parler de tendances plutôt que de lignées génétiques. En outre, Deforge (1985, p.74) précise que « la méthode proposée est familière à ceux qui étudient des phénomènes s'étendant sur de longues périodes : ethnologues, archéologues, économistes », or les sources que nous disposons à propos de l'IMSI catcher s'inscrivent dans une décennie tout au plus. Ainsi, la méthode de Deforge repose sur quelques « époques significatives d'une évolution » ce qui est pratiquement impossible à mettre en place pour l'IMSI catcher, l'objet étant apparu relativement récemment dans l'histoire des techniques d'une part et étant développé et distribué par très peu de constructeurs d'autre part (donc

peu de concurrence et peu de modèles existants) ; à l'inverse d'autres objets techniques tels que la voiture ou le téléphone portable dont l'étude génétique ferait apparaître de nombreuses lignées techniques.

4.2 Des composants de l'IMSI catcher

S'il est donc quasi-impossible à l'heure actuelle d'établir les lignées génétiques de l'IMSI catcher, l'analyse iconographique permet néanmoins de nous renseigner sur les différents composants de celui-ci. Aussi, si les photographies permettent parfois de deviner ces différents composants, les schémas contenus dans les brevets (fig. 35 et 36) et les schémas sur certains sites de vente en ligne permettent d'identifier clairement ceux-ci (fig. 37 à 40). Ainsi se détachent des composants récurrents, à savoir : l'interface radio (récepteur/émetteur), la ou les antennes, l'amplificateur, l'alimentation et l'ordinateur.

L'interface radio

Nous l'avons vu, l'IMSI catcher est un dispositif qui intervient dans le spectre électromagnétique, et plus précisément dans les bandes de fréquences réservées aux communications GSM, c'est-à-dire autour des 900 MHz. Pour pouvoir interagir avec ces fréquences, le dispositif doit être capable d'émettre et de recevoir des ondes radio. Pour ce faire, il a besoin d'une interface RX/TX, RX pour *receiver* (récepteur radio) et TX pour *transmitter* (émetteur radio). Sur la documentation visuelle, celle-ci est la plupart du temps située dans une boîte noire métallique avec des entrées/sorties en façade. Il s'agit en fait de différents composants électroniques soudés à un circuit imprimé.

L'antenne

L'antenne est un des composants nécessaires au fonctionnement de l'IMSI catcher. En effet, elle permet de capter le signal radio et de le transmettre à l'interface radio (RX) et inversement à l'interface radio d'émettre un signal radio (TX). Sa forme dépend directement de la longueur d'onde écoutée : sa forme est donc clairement définie par sa fonction. Elle peut être intégrée directement au dispositif, accrochée à celui-ci ou complètement déportée.

L'amplificateur

L'amplificateur de signal n'est pas toujours nécessaire, mais permet d'augmenter la portée du dispositif, il peut directement intégré à la carte radio ou y être juxtaposé, il est placé entre l'interface radio et l'antenne.

L'alimentation

L'alimentation permet de fournir de l'électricité au dispositif, il en existe deux types : alimentation interne ou externe sur secteur pour les transportables et/ou les embarqués, alimentation sur batterie pour les portables et/ou les embarqués.

L'ordinateur

Dans le corpus, l'ordinateur est le plus souvent dénoté laptop ou notebook.

Il n'apparaît pas toujours sur les images présentées mais il est nécessaire à l'analyse des données ou dans certains cas au fonctionnement même de l'IMSI catcher. En effet, la plupart des IMSI catchers fonctionnent à l'aide d'une technologie appelée Software Defined Radio (SDR) ou radio-logicielle, c'est-à-dire qui repose plus sur une partie logicielle que matérielle. Comme cette technologie nécessite l'exécution d'un programme logiciel, elle repose sur l'utilisation d'un ordinateur. Ainsi, même s'il n'est pas présent visuellement sur les ressources ici présentes, l'ordinateur est toujours quasiment nécessaire à l'interprétation et l'exploitation des données capturées par l'interface radio. L'IMSI catcher peut-être fournit avec une interface graphique (GUI pour Graphical User Interface) qui permet d'afficher et d'interpréter les paquets capturés (et donc les reconstituer en communications) et permet aussi d'exécuter des interactions avec le réseau.

4.3 Du caractère non-concret de l'IMSI catcher et de la pertinence de la reconstitution

Nous avons vu qu'il était difficile d'élaborer une typologie des différents IMSI catchers sur la base des documents à disposition, notamment parce qu'il existe peu de modèles et peu de sources publiques les décrivant, menant à l'impossibilité d'établir des lignées techniques claires. Il est pourtant possible de pressentir certaines d'entres-elles et d'identifier ainsi des tendances. Aussi, on peut observer des degrés de concrétisation plus ou moins élevés en fonction des IMSI catchers. En effet, si on prend l'exemple de l'IMSI catcher portable, celui-ci adopte la forme même du téléphone portable avec l'ensemble des composants intégrés à un boîtier et soudés à la carte mère. De même, l'IMSI catcher intégré à une capsule

aérodynamique présente un degré de concrétisation plus élevé qu'un assemblage de composants embarqués dans un coffre de voiture. Malgré tout, l'IMSI catcher repose généralement sur l'assemblage des composants énoncés précédemment.

En outre, au-delà de l'intégration de l'IMSI catcher en un seul et même objet, la concrétisation de l'objet technique décrite par Simondon s'opère à un autre niveau. En effet, celle-ci relève d'un gain en indivisibilité, que Simondon nomme la « cohérence interne » de l'objet, soit une interdépendance des différents composants entre-eux ; ce qui permet, paradoxalement, l'apparition de nouvelles fonctions et entraine la simplification de l'objet qui se spécialise. Autrement dit dans le cas l'IMSI catcher : l'apparition de plusieurs fonctionnalités uniquement dédiées à l'écoute du réseau téléphonique entraînant par là même une simplification de l'objet, et qui en ferait un objet dont la fonction serait strictement réservée à cet effet.

Or, pour l'IMSI catcher ses composants sont toujours « individualisables » ou « désagrégeables » ; à la différence du moteur thermique à combustion interne ou de la turbine Guimbal présentés par Simondon. Comme on peut particulièrement le voir sur les schémas de fonctionnement présents dans les brevets, il s'agit là d'un assemblage dans lequel chacun des éléments accomplit une tâche donnée et communique son résultat avec l'autre plutôt que d'un tout indivisible fonctionnant de manière autonome. Ainsi, tous les composants susmentionnés conservent leur indépendance et continuent à être fonctionnel lorsqu'ils sont dissociés : l'ordinateur peut toujours accomplir d'autres tâches une fois séparé du tout, il en est de même pour l'alimentation qui pourra toujours alimenter d'autres appareils ou de l'antenne qui pourra toujours capter et transmettre des signaux à d'autres interfaces. C'est pourquoi on pourrait qualifier l'IMSI catcher d'« agrégat technique » ou de « dispositif technique relevant d'un assemblage d'objets techniques » plus que d'un objet technique, au sens Simondonien du terme.

Enfin selon Simondon, l'objet technique au paroxysme de sa concrétisation entre dans une phase d'« individualisation » dans laquelle il n'a plus besoin d'auxiliaire humain pour s'accomplir enfin comme un véritable « individu technique », or dans tous les cas étudiés dans ce chapitre, l'IMSI catcher ne peut se défaire d'un opérateur humain. N'oublions pas que pour appliquer pleinement la démarche Simondonienne il est nécessaire de prendre l'objet dans son évolution et non pas séparément, et comme nous avons pu le voir plus tôt c'est une tâche délicate étant donnée l'apparition relativement récente de l'IMSI catcher ainsi que le peu d'abondance de modèles inventoriés. Il faudra peut-être attendre quelques décennies pour voir une évolution que l'on pourra étudier sous le prisme des lignées techniques, ou peut-être l'IMSI catcher n'évoluera-t-il jamais en ce sens au vu de la disparition actuelle de la 2G au profit de la 5G. N'oublions pas non plus que la concrétisation d'un objet technique décrite par Simondon s'étudie aussi à travers

l'analyse de ses effets sur ses milieux associés ; or, ces milieux sont ici principalement ceux des concepteurs et des utilisateurs de l'IMSI catcher (autrement dit les surveillants) et il y a dans le caractère sécuritaire et confidentiel voire secret de l'objet une difficulté à les approcher.

Ainsi, devant l'impossibilité d'établir une chronologie et la difficulté à étudier le dispositif étudié (pour des questions de coût notamment comme on peut le voir dans la documentation technique), il apparaît tout à fait pertinent d'adopter comme alternative une démarche de recherche-création en se plaçant comme concepteur et designer plutôt qu'en tant qu'historien des techniques. Au-delà du regard observateur de Simondon et de Deforge, il semble plus pertinent d'adopter une approche de création dans le cas de l'IMSI catcher où le manque de ressources constitue un frein à son étude. Dans ces conditions, et comme nous l'avons vu dans le chapitre précédent, une approche méthodologique adéquate peut être celle de la reconstitution, c'est celle-ci que je mettrai à l'œuvre dans le chapitre suivant.

Key Features

- Covertly identify the unique identity (IMSI/IMEI/TMSI) of GSM cell phones
- Locate known targets using their GSM mobiles (in conjunction with DF equipment)
- Take control of target phones for the purpose of denying GSM service
- Create exclusion zone to deny GSM network coverage (subject to export license approval)
- Intercept SMS messages sent by a target
- Multiple BTS system allowing up to 2 BCCH on 1 network or 2 BCCH on 2 different networks
- Blind/Silent call up to 7 target cell phones per BTS

Specifications

The GSM-XPZ family of active interception solutions provides a tactical tool for law enforcement, government and military agencies.

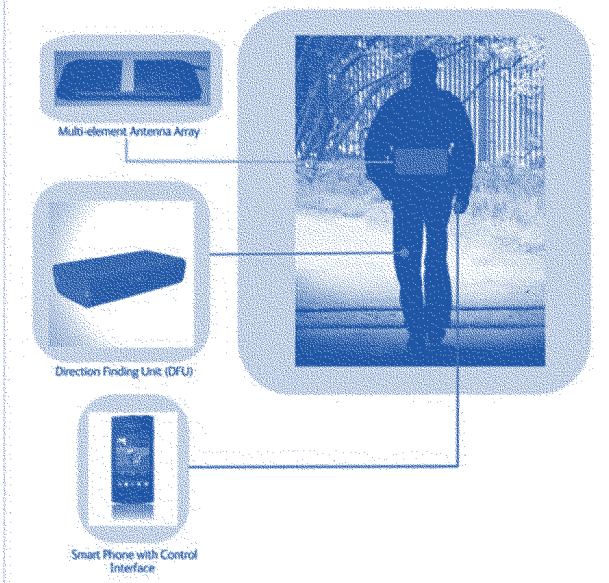
Utilising commercial base-station technology and operating independently of the GSM network providers, the GSM-XPZ family of vehicle and portable products provide the capability to clone and simultaneously transmit multiple fake GSM networks to interact with the GSM Cell Phones.

Physcial	
Size:	W 280mm x H 70mm x D 290mm,
Weight	4.43Kg
Interface Connections:	Antenna Ports: 1 x Combined Tx, 1 x Combined Rx, 1 x WiFi
Technical	
Channels:	2 Channels 1 x 900 + 1 x 1800 or 1 x 850 + 1 x 1900
Channel Range:	Euro: E-GSM, GSM, DCS US: 850, PCS
Channel Bandwidth:	200KHz
Output Power:	1mW to 2W (max) per channel
Data:	Interface via secure Ethernet or WiFi
Environmenal	
Operating Temperature:	-5°C to +45°C
Storage Temperature:	-10°C to +70°C
Power	
Power Consumption (Max):	70W
Power Supply:	12Vdc

Portables

Fig.16. *Cobham Tactical Communications and Surveillance Catalogue*. 2014. Capture d'écran.

Deployment Example



Key Features

- Allows direction finding of UMTS and GSM devices
- Resolves target location to within a few metres
- Direction Finding Unit (DFU) is controlled by smart phone over Bluetooth (wireless)
- Choice of multiple feedback mechanisms
- Can DF on BTSs and Node Bs, in addition to target mobile devices.
- Covert body-worn antenna pack included
- Compatible with multiple antennas for different scenarios
- Audio feedback mode allows for covert operation
- DFU protocol and frequency configuration is software adjustable to user requirements

Specifications

The Evolve4 Hand Held Direction Finder (Evolve4-HHDF) is a light-weight, portable, state of the art device for tracking and geo-locating cell phones.

The Evolve4-HHDF works with the 3GN's 3G Blind Call feature to allow tracking of UMTS devices. It is also backwards compatible with GSM.

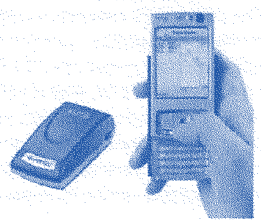
The Evolve4-HHDF is controlled by a smart phone connected to the unit over a Bluetooth link. This makes the unit easy to configure and use without attracting attention.

The Evolve4-HHDF features multiple feedback mechanisms to cater for a variety of mission scenarios. Choose from visual or audio feedback depending on the operational requirement.

Function:	Provides RF signal strength indication on a selectable UARFCN/ARFCN
Frequency Range (MHz)	
GSM	**UMTS**
850 Band	Bands I
900 Band (inc E-GSM)	II
1800 Band	III
1900 Band	IV
	V
	VIII
Size (mm)	DFU: 120(l) x 65(w) x 28(d) High band antenna: 78(l) x 78(w) x 18(d) Low band antenna: 120(l) x 120(w) x 17(d)
Weight (grams)	DFU: 140g High band antenna: 230/460 (element/array) Low band antenna: 550/1100 (element/array)
Power	3 x AA batteries
Battery Life (DFU)	Circa 3 hours (typical usage)
Antenna	4 x patch antennas in configurable array
Interfaces	On/Off, Status LED, Smart phone interface

Fig.17. *Cobham Tactical Communications and Surveillance Catalogue*. 2014. Capture d'écran.

Nemo Handy (N95)



Capabilities

Description:
•Cellular Survey Tool for testing mobile applications QoS/QoE and measuring the air interface of EGSM/ GPRS/ EDGE/ WCDMA/ HSDPA/ Wi-Fi 802.11/g wireless networks. It is complete with voice and video streaming quality MOS testing, cell and timeslot testing, and full application level metrics on voice and video calls.

Limitations & Planning Factors

Nemo-Handy Equipment Specifics:
- Can only record one network at a time
- Easy to conceal, although HS is not typical size/shape
- When the program is running, easy to see on the HS screen
- Does not give extended BA list

Vendor:
Protocols: HSDPA/WCDMA 2100, GSM/EGSM/GPRS/EGPRS 850/ 900/ 1800/ 1900
BOIP:
Cost: approx $11,500.00

Approval: Title 10

SECRET // NOFORN

Nemo Outdoor

CAPABILITIES

- •Cellular Survey Tool
- •System includes
  - •2 GSM HS
  - •1 CDMA HS
  - •1 TDMA HS
  - •Assorted Scanners
  - •GPS Receiver
- Records cellular information for download to NEMO Analyze
- Can hook DTI scanners to laptop for simultaneous recording of numerous networks

LIMITATIONS & PLANNING FACTORS

Nemo Outdoor Equipment Specifics:
- Must be hooked to a laptop
- Using entire system can be cumbersome and difficult to conceal
- Does not give extended BA list
- Capable of running simultaneous multiple protocol survey

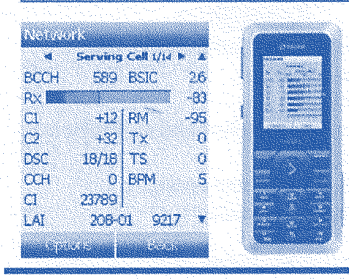
VENDOR:
PROTOCOLS: 900Mhz, 1800, 850, 1900, CDMA
BOIP:
COST: Approx $80,000.00

APPROVAL AUTHORITY FOR USE: Title 10

SECRET // NOFORN

Fig.18. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran. /
Fig.19. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran.

Sagem OT488, 498



Capabilities

Description:
•Cellular Survey Tool Cellular Survey Tool for measuring the air interface of GSM/ EGSM/ GPRS wireless networks.

Limitations & Planning Factors

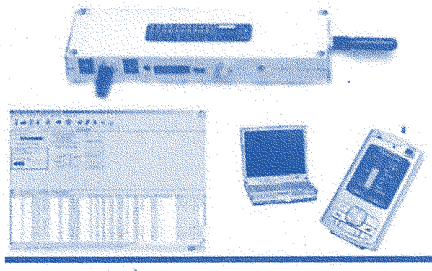
Sagem Equipment Specifics:
•Can only record one network at a time
•Easy to conceal when not hooked to laptop
•When the program is running, easy to see on the HS screen
•Does not give extended BA list

Vendor:
Protocols: 850, 900, 1800, and 1900Mhz
BOIP: Part of MRT systems
Cost: approx $10,000.00

Approval: Title 10

SECRET // NOFORN

Blackfin I/II



Capabilities

Description: BLACKFIN II adds more performance and capability to the Blackfin system while keeping the same compact package. BF II is designed to body worn or packaged for concealed missions. Can be discretely configured and controlled via blue tooth with the Mobile controller. Quad Band interrogator that can conduct passive monitoring, survey, Interception of GSM voice and SMS of a preloaded target lists, blanketed or targeted denial of service, and geo a given GSM handset.

Limitations & Planning Factors

Blackfin Equipment Specifics:
• Supported Bands: Model A (900/1800MHz)
• Model B (800/1900MHz)
• Low power for battery operation
• USB or Bluetooth connection
• Mobile controller provides limited control
• 5-7 hour battery life

Vendor: Harris Corporation Wireless Products Group
Protocols: GSM 850, 900, 1800, 1900

BOIP:
Cost: $75,000.00

Approval: Title 10

SECRET // NOFORN

Fig.20. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran. /
Fig.21. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran.

Specifications

The 3G-N is a state-of-the-art multi-channel 3G / UMTS (WCDMA) tactical active interception solution. The 3G-N is currently used in conjunction with the GSM-XPZ range. Control is streamlined to a single interface where users can simultaneously acquire the identities of GSM and UMTS phones.

For geo-locating and tracking purposes the UMTS target phone is 'pushed' onto the GSM-XPZ cell and then placed into blind call mode.

Physcial	
Size:	W 324mm x H 180mm x D 398mm
Weight:	16.5Kg (20Kg including carry case)

Technical	
Function:	• Acquire the identify parameters (IMSI, IMEI & TMSI) of UMTS cell phones off-air from two different UMTS networks simultaneously • 'Push' target cell phones to GSM in a controlled manner for geo-locating • Correctly interact with non-target cell phones to preserve 3G network service in the operational zone
Channels:	Two (2)
Channel Range:	UMTS Band 1 (2110-2170MHz)
RF Output Power:	2 x 5W max or 1 x 20W max
RF Output Connector:	3 x N Type

Power	
Power Supply:	12Vdc - 24Vdc
Power Consumption:	16A, 400W maximum

Environmental	
Operating Temperature:	-5°C to +45°C
Storage Temperature:	-10°C to +70°C

Specifications

The new Evolve4-Nimbus from Cobham is a state of the-art multi-channel tactical active interception solution.

The Evolve4-Nimbus is frequency and protocol agile. Frequency agility across 6 common frequency bands allows maximal operational flexibility.

Protocol agility allows a variety of protocols to be supported. UMTS capability will be provided at launch, with GSM and LTE to follow subsequently.

The Evolve4-Nimbus is rugged by design and suitable for deployment across a wide range of operational environments.

The Evolve4-Nimbus is compatible with the GSM-XPZ product range. Control is streamlined to a single interface where users can simultaneously acquire the identities of GSM and UMTS phones.

For geo-locating and tracking purposes, UMTS target phones can be held in native UMTS(3G) blind call or 'pushed' onto a GSM-XPZ cell and then placed into GSM blind call.

Fig.22. *Cobham Tactical Communications and Surveillance Catalogue*. 2014. Capture d'écran. / Fig.23. *Cobham Tactical Communications and Surveillance Catalogue*. 2014. Capture d'écran.

Key Features

- Take control of target phones for the purpose of denying GSM service
- Create exclusion zone to deny GSM network coverage (subject to export license approval)
- Intercept outgoing calls and SMS messages
- Rugged form factor for in-vehicle use
- Multiple BTS system allowing up to 4 BCCH on 1 network or 4 BCCH on 4 different networks
- High transmit output power - up to 50 Watts
- Blind/Silent call up to 7 target cell phones per BTS
- Simultaneous intercept of up to 4 outgoing voice calls

Specifications

The GSM-XPZ family of active interception solutions provides a tactical tool for law enforcement, government and military agencies.

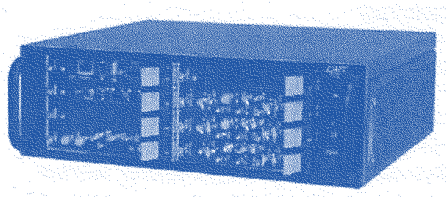
Utilizing commercial base-station technology and operating independently of the GSM network providers, the GSM-XPZ family of vehicle and portable products provide the capability to clone and simultaneously transmit multiple fake GSM networks to interact with GSM cell phones.

Physcial	
Size:	W 500mm x H 200mm x D 580mm
Weight	28Kg
Interface Connections:	Antenna Ports: Directional: 2 x Low Band, 2 x High Band Omni: 2 x Combined Data/Audio: Interface via secure Ethernet
Technical	
Channels:	4 Channels 2 x 900 + 2 x 1800 or 2 x 850 + 2 x 1900 or 1 x 850 + 1 x 900 + 1 x 1800 + 1 x 1900 (Quad)
Channel Range:	Euro: E-GSM, GSM, DCS US: 850, PCS Quad: 850, E-GSM, GSM, DCS, PCS
Channel Bandwidth:	200 KHz
Output Power:	1mW to 50W (max) per band
Power	
Power Consumption (Max):	600W
Power Supply:	24 Vdc
Environmenal	
Operating Temperature:	-5°C to + 45°C
Storage Temperature:	-10°C to +70°C

Fig.24. *Cobham Tactical Communications and Surveillance Catalogue*. 2014. Capture d'écran.

Transportables

DRT 1101B



Capabilities

Description: The DRT 1101B provides a compact, yet powerful, surveillance capability against a variety of analog and digital wireless standards. The DRT1101B can be configured to support DF, digital voice intercept/recording, supports target lists of up to 10,000 entries, and has a flexible tuner configuration which provides frequency coverage of all bands of interest. Up to four tuners can be incorporated in unit.

Limitations & Planning Factors

DRT 1101B Equipment Specifics:

Maximum Number of Channels: 96 (half-duplex)
48 (full-duplex)

Frequency Coverage:
0.2 MHz - 3000 MHz

Compatible with: Windows 2000, XP

Audio Outputs:
16-Channel Analog
16-Channel Internal Digital Recorder
Stereo Headphones
E1 Audio (optional)

Controlled from PC using Windows 2000/XP via Ethernet interface.

User-friendly Graphical User Interface (GUI)

Integrated spectrum analysis tool

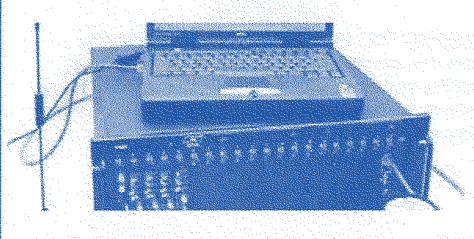
Vendor: Digital Receiver Technologies
Protocols: Multi-protocol
BOIP:
Cost: $78,850.00

Approval: Title 10/ 50

SECRET // NOFORN

DERIVED FROM:
DATED: 01 May 2006
DECLASSIFY ON: 07 January 2034

DRT 1201C



Capabilities

Description: The DRT 1201C provides a compact, yet powerful, surveillance capability against a variety of analog and digital wireless standards. The DRT1201C can be configured to support DF, digital voice intercept/recording, supports target lists of up to 10,000 entries, and has a flexible tuner configuration which provides frequency coverage of all bands of interest. Up to four tuners can be incorporated in unit.

Limitations & Planning Factors

DRT 1201C Equipment Specifics

- Monitors up to 544+ half-duplex channels (32+ channels per WPM3).
- Software configurable to process various wireless standards.
- Processes multiple formats simultaneously.
- DF option available.
- Flexible tuner configuration provides frequency coverage of all bands of interest.
- RFT3: Dual channel transceiver VHF/UHF coverage from 2-3000 MHz; HF from 0.5 - 32 MHz
- HFT1: High performance HF receiver from 0.2-30 MHz
- MUT1: Microwave receiver from 0.2-8.5 GHz
- FPGA based Wireless Processor, WPM3, enables wideband signal processing. Can also generate 32+ narrowband signals.

Vendor: Digital Receiver Technologies
Protocols: Multi-protocol
BOIP:
Cost:

Approval: Title 10/ 50

SECRET // NOFORN

DERIVED FROM:
DATED: 01 May 2006
DECLASSIFY ON: 07 January 2034

Fig.25. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran. /
Fig.26. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran.

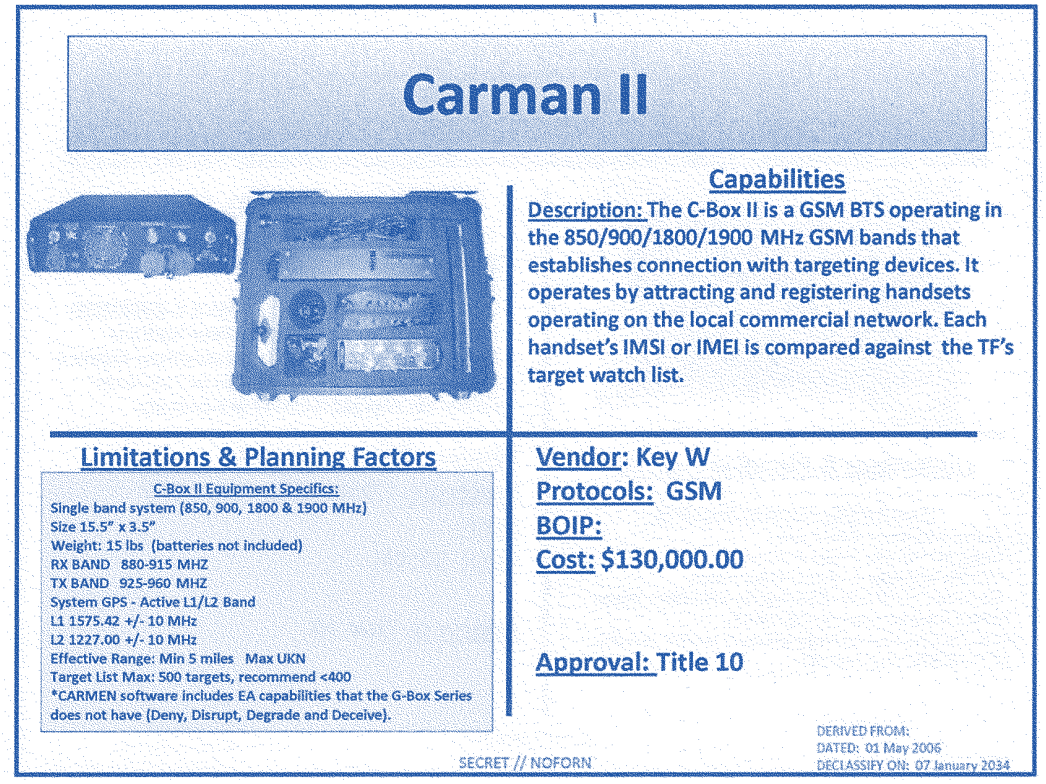


Fig.27. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran.

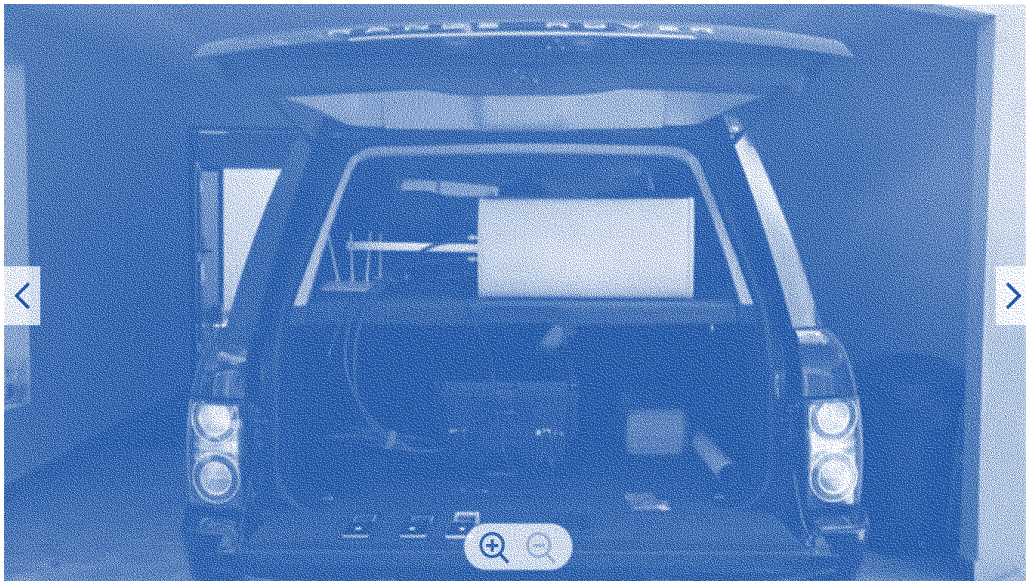


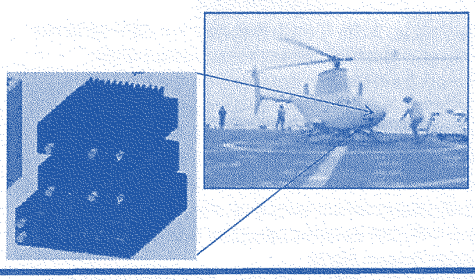
Fig.28. Résultat de la recherche ‘IMSI catcher’ sur alibaba.com. 2021. Capture d’écran.

Fig.29. Résultat de la recherche ‘IMSI catcher’ sur alibaba.com. 2021. Capture d’écran.

Fig.30. Résultat de la recherche ‘IMSI catcher’ sur alibaba.com. 2021. Capture d’écran. / Fig.31. Résultat de la recherche ‘IMSI catcher’ sur alibaba.com. 2021. Capture d’écran.

SECRET

Twister – Firescout APG



Capabilities

Description: Twister is a multi-frequency band, micro-class Base Station Router. Its has a power output of +43dBm, integrated GPS, Voice & High-speed Data capability, GSM security & encryption making system highly mobile and deployable for field use. The system is designed for VBTS GUI Software support which includes full VBTS GUI feature base and applications. The software allows for complete command and control, which provides support for a variety of field applications. The system is optimized for low power consumption, custom installation, and familiarity of use w/ existing VBTS GUI operators.

Specifications:

Physical Dimensions:
- Twister BSR: 9.38"L x 7.75"W x 2.13" H
- Twister Aux Front-End: 8.25"L x 5.75"W x 3.25"H

Weight
- Twister BSR = ~ 3.5 lbs
- Twister Aux Front-End: ~ 6.5 lbs

Environmental
- Operating Temp: 0° to + ~ 50°C (90% humidity non-condensing)
- Storage Temp: -30°C to + ~80°C
- Convection cooled

GSM Frequency Capabilities
- EGSM (900Mhz), DCS (1800Mhz), PCS (1900 Mhz)
- Full-rate Voice Encoder, Basic SMS Messaging

Power:
- Input Power Requirements = 55W (Max) in typical configuration
- Input Voltage Range = 28 VDC

Integrator: Northrop Grumman IS/AS ICW PMA-266
Protocols: GSM 900/1800/1900 Mhz
Approval Authority: GFC IAW host nation GCC approvals

SECRET // NOFORN
SECRET

SECRET

BLOS Pod

Capabilities

Description: Pod based capability that allows for remote operation of Ethernet payloads removing the requirement for dedicated, line-of-sight (LOS) tactical data link. Ethernet data is routed over the aircraft's serial SATCOM data link using an Asymmetric Ethernet Device (AED). The AED is placed on each end of the aircraft's SATCOM data link (onboard Pod, GCS) and is used to convert Ethernet data to serial for transit across the link.

Equipment Specifics:
- AWR completed for USSOCOM MQ-1/9 aircraft, Warrior Blk-0
- Pod weight: ~123 lbs (with G-Box/WJ payloads)
- Bandwidth requirements: Typical configuration, 4800 bps uplink, 256 kbps downlink
- Current Payloads: Garuda (G-Box), Windjammer-U
- Payload Vendor(s): Protected, SR Technologies

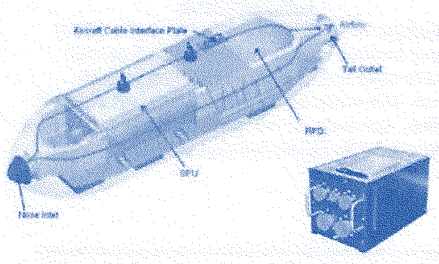
Integrator: Northrop Grumman IS ICW General Atomics
Protocols: GSM 900/1800, Thuraya/Inmarsat
Approval: Ground Force Commander IAW host nation GCC approvals

SECRET // NOFORN
SECRET

Fig.32. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran. /
Fig.33. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran.

SECRET

Traveler Pod – T-Pod



Capabilities

Description: Pod based software defined multi-protocol system capable of GSM survey/map/geo-location, CDMA survey/map geo-location, HPCP/PTT intercept/DF, Thuraya intercept/copy/geo-location. Traveler's less instrusive techniques reduces network signature/impact on the network. Provides robust airborne network survey capability.

Equipment Specifics:

- In development for USSOCOM Warrior Blk-1
- 5-35 awaiting 3U Traveler variant prior to Pod integration
- Pod weight : ~180 lbs (with payloads)
- Current Payload (s): Traveler 6U (Warrior)
- Payload Vendor(s): BAE Systems

Integrator: BAE Systems ICW General Atomics

Protocols: GSM, CDMA, Thuraya, HPCP/PTT, TTL

Approval: Ground Force Commander IAW host nation GCC approvals

SECRET // NOFORN

SECRET

Fig.34. *Government Cellphone Surveillance Catalogue*. 2015. Capture d'écran.

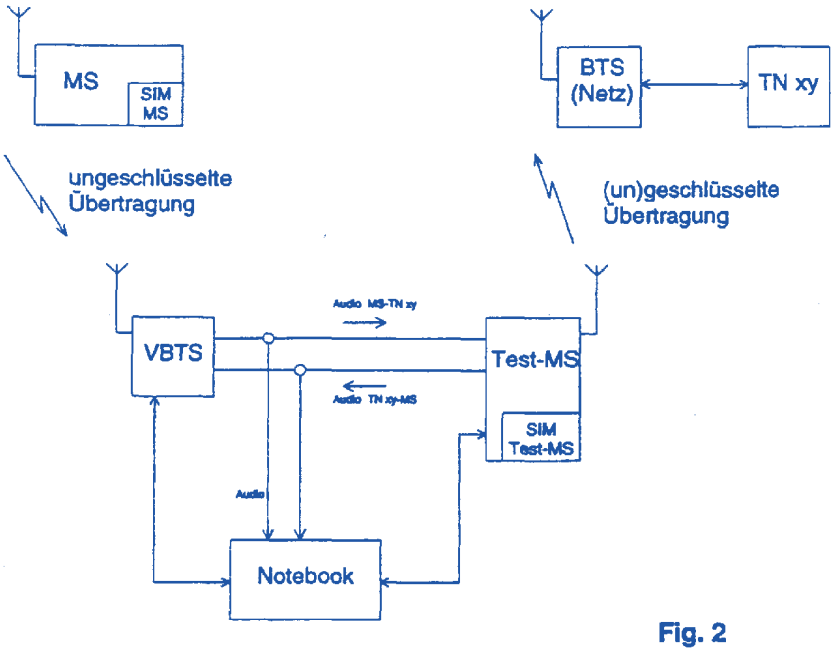


Fig. 2

Schémas

Fig.35. Rohde & Schwarz. Brevet EP1051053A2·2000-11-08 «Procédé pour identifier un utilisateur d'un téléphone mobile ou pour écouter les appels émanants». 2000. Capture d'écran.

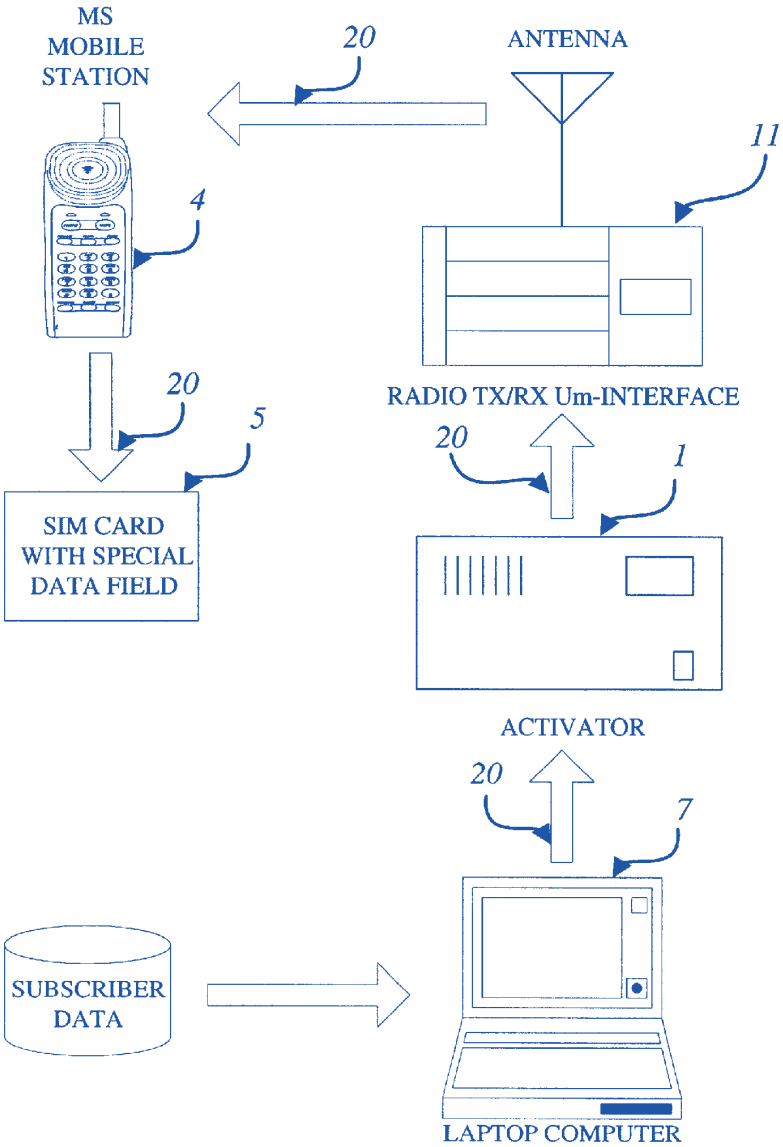


FIG.3

Fig.36. Peter Suprunov. Brevet US6405030B1 «System for interception of digital cellular phone communication». 1999. Capture d'écran.

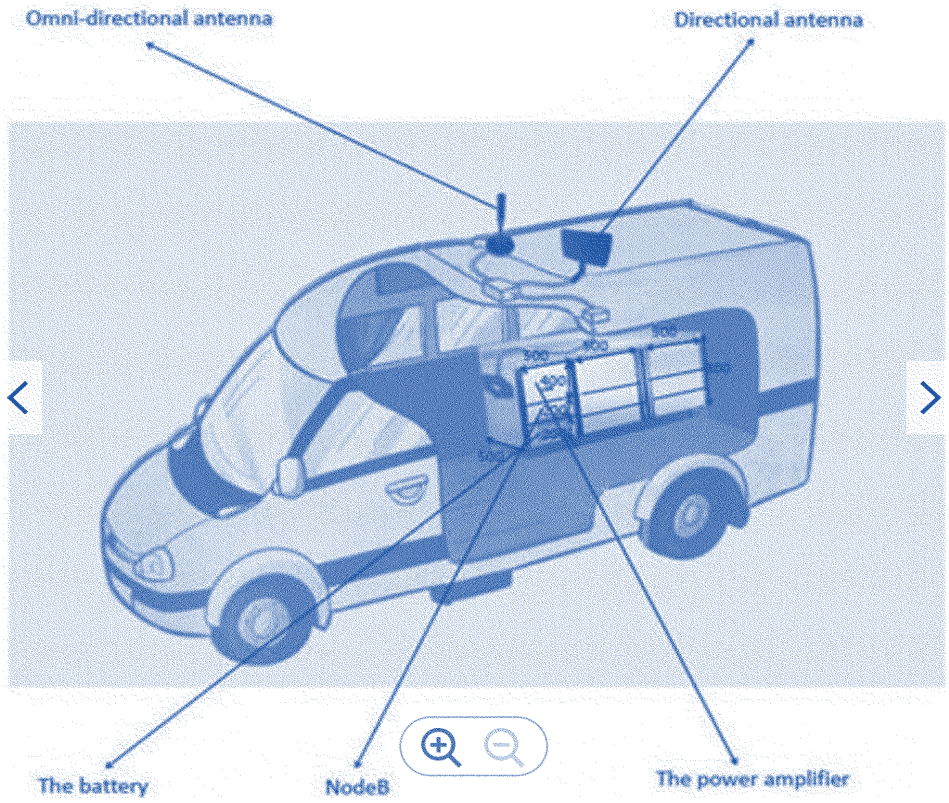
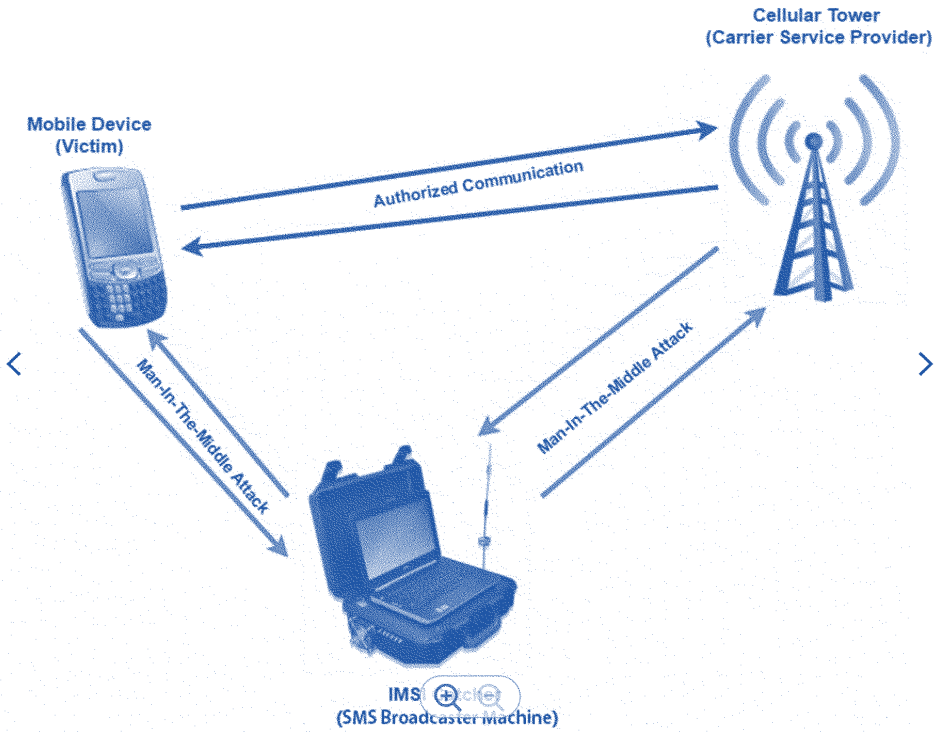


Fig.37. Résultat de la recherche ‘IMSI catcher’ sur alibaba.com. 2021. Capture d’écran. / Fig.38. Résultat de la recherche ‘IMSI catcher’ sur alibaba.com. 2021. Capture d’écran.



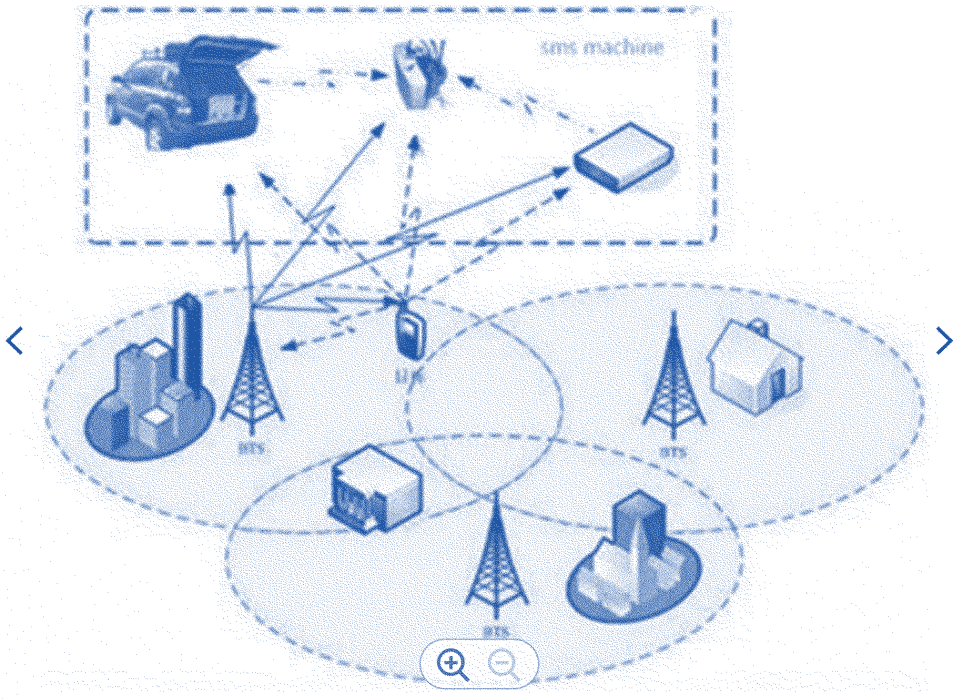


Fig.39. Résultat de la recherche ‘IMSI catcher’ sur alibaba.com. 2021. Capture d’écran. / Fig.40. Résultat de la recherche ‘IMSI catcher’ sur alibaba.com. 2021. Capture d’écran.

Fig. 41. GSM Interceptor. Milipol 2019. Photo: Marta Revuelta.

Fig. 42. GSM Interceptor. Milipol 2019. Photo : Marta Revuelta.

Fig. 43. IMSI catcher. Milipol 2019. Photo: Marta Revuelta.

Fig. 44. Véhicule d'intervention embarquant des antennes, potentiellement à des fins d'interception GSM. Milipol 2019. Photo : Marta Revuelta.

Fig. 45. Différents types d’antennes. Milipol 2019. Photo : Marta Revuelta.

5
Recherche par le design I : Refaire un IMSI catcher[47]

47 Ce chapitre a fait l'objet d'une publication dans la revue continent. *Issue 8.1-2 / 2019*, dont le thème était *Apocryphal technologies*. Le concept de technologie apocryphe proposé par Jamie Allen est particulièrement pertinent dans le cas de l'IMSI catcher. En effet, comme nous avons pu le voir précédemment, le dispositif d'interception est largement entouré de mythes et de pré-suppositions quant à ses capacités ainsi qu'à ses usages. Questionner cette dimension apocryphe permet « d'exposer les représentations erronées (involontaires ou intentionnelles) et les mauvaises interprétations (naïves ou délibérées) qui entourent les développements technologiques. » Toutefois, dans le cadre de la thèse je ne reprendrai pas à mon compte ce caractère apocryphe de l'objet en question et je préfère le désigner comme un objet confidentiel ou encore lui prêter une nature secrète consubstantielle.

Devant la difficulté d'étudier l'IMSI catcher sur la base d'un corpus d'éléments visuels une question se pose : comment, en tant que chercheurs, pouvons-nous étudier une technologie aussi confidentielle ? Jentery Sayers défend la pertinence de refaire ou reconstituer — *remaking* — d'anciennes technologies dans les media studies et les *digital humanities* (Sayers, 2014). Plus précisément, il a développé une typologie dans laquelle il décrit différents niveaux d'implication pour lesquels le processus du refaire est pertinent, à savoir : « composition », « assemblage », « interface », « échec », « abstraction », « instrumentalisme » et « spéculation ». Bien que l'IMSI catcher soit une technologie actuelle et contemporaine plutôt qu'une technologie passée, il existe peu de ressources sur la façon dont il fonctionne et beaucoup de spéculations émergent autour de ce qu'il est capable d'accomplir. Ainsi, un moyen de traiter le caractère confidentiel de l'IMSI catcher est de le reconstruire à travers un processus itératif de design à l'aide d'éléments logiciels et matériels. Face au manque de ressources autour des IMSI catchers et de leur design, ce qui soulève des enjeux de transparence et contribue à son caractère confidentiel ; ce chapitre présente (1) les différentes versions d'IMSI catchers que j'ai reconstituées ; et (2) discute la pertinence d'une telle méthode en rapport à l'approche historique de Sayers pour une technologie confidentielle. Enfin (3), je m'intéresse à la pertinence de la reconstitution au regard de méthodes de design spéculatif pour traiter de tels objets.

5.1 Le processus de reconstitution

La source d'information la plus importante pour la reconstitution se trouve au sein de communautés open source telles que Osmocom (Open source mobile communications), OpenBTS et YateBTS qui visent à substituer les systèmes propriétaires complexes avec des outils et des logiciels ouverts et à fournir une documentation et des tutoriels pour construire des sites femtocellulaires ou picocellulaires dans des zones non couvertes par le réseau GSM. Aussi, des programmeurs indépendants et des hackers mettent en ligne des scripts afin de démontrer l'utilisation d'IMSI catchers et de les reconstruire « pour mieux comprendre l'infrastructure GSM ». Ce sont les sources d'information principales qui ont été utilisées pour produire les prototypes suivants.

Le processus de reconstruction peut informer sur ce que la technologie est réellement et comment elle opère ; c'est aussi une manière d'interroger les limites du dispositif afin d'exposer les représentations erronées qui l'entourent, tester des hypothèses, et discuter son caractère confidentiel. Pour ce faire, j'ai tout d'abord parcouru des bases de données de code logiciel (comme Github), sur lesquelles des programmeurs mettent en ligne des logiciels permettant de comprendre comment les IMSI catchers fonctionnent ; puis j'ai parcouru la documentation fournie par les communautés open source citées précédemment,

celle-ci oriente notamment sur le matériel à posséder afin de pouvoir exécuter les logiciels qu'elles distribuent. Après consultation de ces différentes sources, j'ai pu identifier deux grandes familles d'IMSI catchers : les IMSI catchers passifs et les IMSI catchers actifs.

Passif vs actif

Les IMSI catchers fonctionnent sur deux modes différents : un mode passif et un mode actif. Dans le mode passif, l'IMSI catcher « n'attrape » pas à proprement parler les *International Mobile Subscriber Identities*, mais les observe plutôt. Il « écoute » l'activité du réseau en continu et recherche les IMSIs en clair (envoyés par les téléphones lorsqu'ils se connectent à l'antenne relais) et n'interfère pas avec cette activité. Un dispositif passif fonctionne sur une zone définie qui correspond à la couverture de l'antenne relais (aussi désignée par le terme de cellule), le dispositif obtiendra ainsi l'identité des téléphones présents dans cette cellule.

Dans le mode actif, l'IMSI catcher réplique l'activité d'une cellule, il peut usurper l'identité d'une antenne relais existante ; ainsi les téléphones mobiles qui se trouvent à sa portée s'y associent en toute transparence pour l'utilisateur (c'est une attaque de l'homme du milieu). Un dispositif actif fonctionne localement sur une zone définie par sa puissance d'émission (le plus puissant, plus grande sera la zone). S'il n'est pas connecté à l'infrastructure GSM existante (mode local), il n'est pas capable de relayer des appels téléphoniques sortants ou des messages textuels vers l'extérieur ; il est seulement capable d'attraper les IMSIs des téléphones associés et de passer des communications entre eux. S'il est connecté à l'infrastructure GSM existante (à une antenne relais légitime), il est capable de rediriger le trafic sortant et en forçant le non-chiffrement des communications, il est capable d'intercepter des appels téléphoniques et des messages textuels.

Deux prototypes passifs a.k.a. *Moto et Real*

La première version d'un IMSI catcher passif que j'ai reconstituée fonctionne avec osmocomBB — une implémentation logicielle GSM libre et ouverte fonctionnant sur un ordinateur portable sous Ubuntu et un téléphone compatible : dans les cas présents un Motorola C118, un téléphone à 30$ programmable à l'aide d'un câble USB dédié (fig. 46). En exécutant le firmware[48] *osmocom* dédié sur le téléphone portable, il est possible de lui faire accomplir des tâches spécifiques. Dans ce cas, il est possible de forcer le téléphone à écouter l'activité d'une antenne relais désignée. Décoder et filtrer le trafic entrant permet d'isoler les *paging requests*

48 Programme intégré dans un matériel informatique pour qu'il puisse fonctionner.

Fig. 46. *MOTO*: ordinateur portable, téléphone Motorola C118, câble USB.

(émises lorsque les téléphones tentent de s'authentifier auprès de l'antenne-relais) qui contiennent l'IMSI des téléphones requérants en clair (fig. 47).

La seconde version d'un IMSI catcher passif que j'ai reconstituée est basée sur une puce Realtek RTL2832U — habituellement trouvée sur des tuners USB DVB-T, vendus sur Internet autour de 10$ pour regarder la télévision numérique — et un ordinateur portable sous Ubuntu (fig. 48). En utilisant la radio logicielle (en anglais *software-defined* radio ou SDR) comme le permet le logiciel *gqrx*, il est possible d'utiliser ce *dongle* pour scanner les bandes de fréquences GSM. C'est aussi ce que la suite logicielle gr-gsm permet de faire : dans un premier temps « grgsm_scanner » scanne les alentours à la recherche d'antennes-relais (fig. 49) puis « grgsm_livemon » écoute la fréquence d'émission de l'antenne-relais choisie (fig. 50). Les données acquises avec « grgsm_livemon » sont ensuite interprétées avec l'aide du script Python « simple_IMSI-catcher.py » fourni par Oros42 sur Github[49] (fig. 51). Comme dans la configuration précédente avec osmocomBB et le Motorola C118, le script Python recherche les *paging requests* qui contiennent les IMSIs en clair.

Comme leur nom le laisse supposer, ces dispositifs passifs n'ont pas la capacité d'interférer avec leur environnement, ils sont dans un mode d'écoute qui permet déjà d'informer sur celui-ci. Malgré l'utilisation d'algorithmes de chiffrement (à savoir A5/1 et A5/3) pour protéger les communications (appels téléphoniques, messages textuels), l'IMSI est toujours transmis en clair dans le processus d'authentification. Comme l'IMSI est un identifiant unique, ces attaques passives fournissent assez d'information pour discriminer un utilisateur dans une cellule donnée. À partir du MCC et du MNC, le script donne le pays d'origine et l'opérateur téléphonique du téléphone intercepté, il est ainsi possible d'obtenir des « images » de différentes localisations. Par exemple, les dispositifs reconstitués ont été testés dans trois villes différentes : à Genève en Suisse, qui est une ville très cosmopolite (en partie à cause des organisations internationales), les dispositifs ont intercepté des IMSI d'origines diverses ; à l'inverse, à Mourmansk ou Saint-Pétersbourg en Russie[50], les dispositifs ont intercepté des IMSI russes ou ukrainiens uniquement. Les dispositifs décrits précédemment sont capables d'écouter une seule bande de fréquence à la fois, mais il est possible de configurer plusieurs dispositifs à la fois afin d'obtenir un IMSI catcher multibande.

49 <https://github.com/Oros42/IMSI-catcher> consulté le 15.02.2022

50 Les dispositifs ont été testés en Suisse mais aussi en Russie à l'occasion des festivals d'art numérique *Inversia 2019* et *Cyfest 2019*.

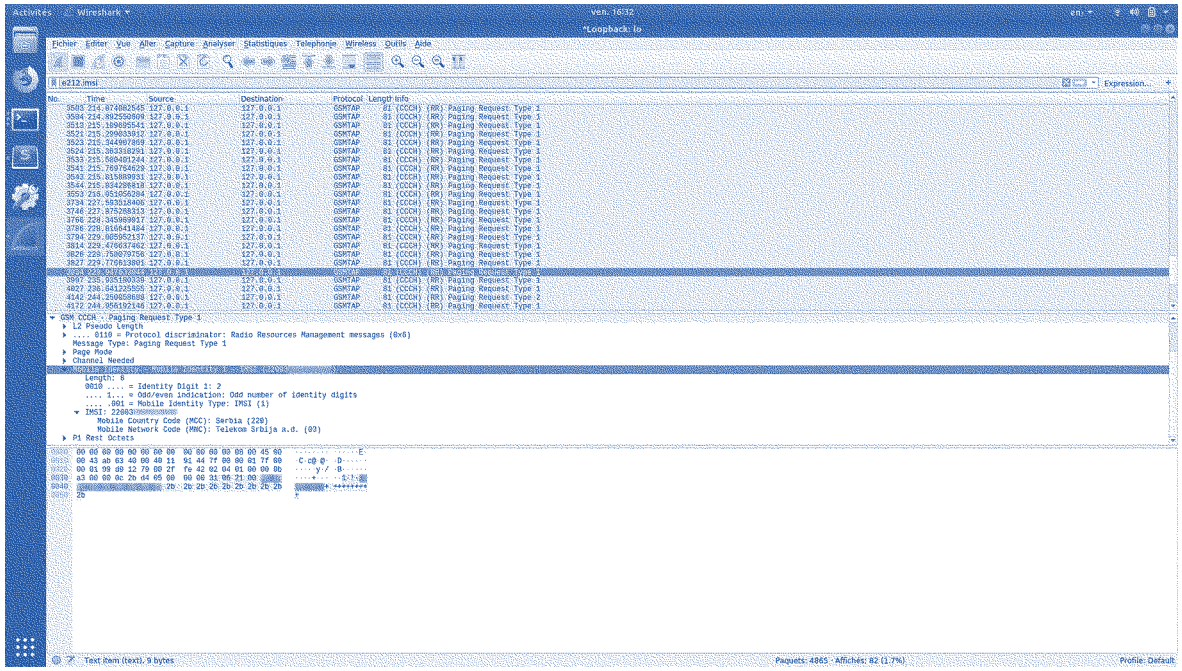
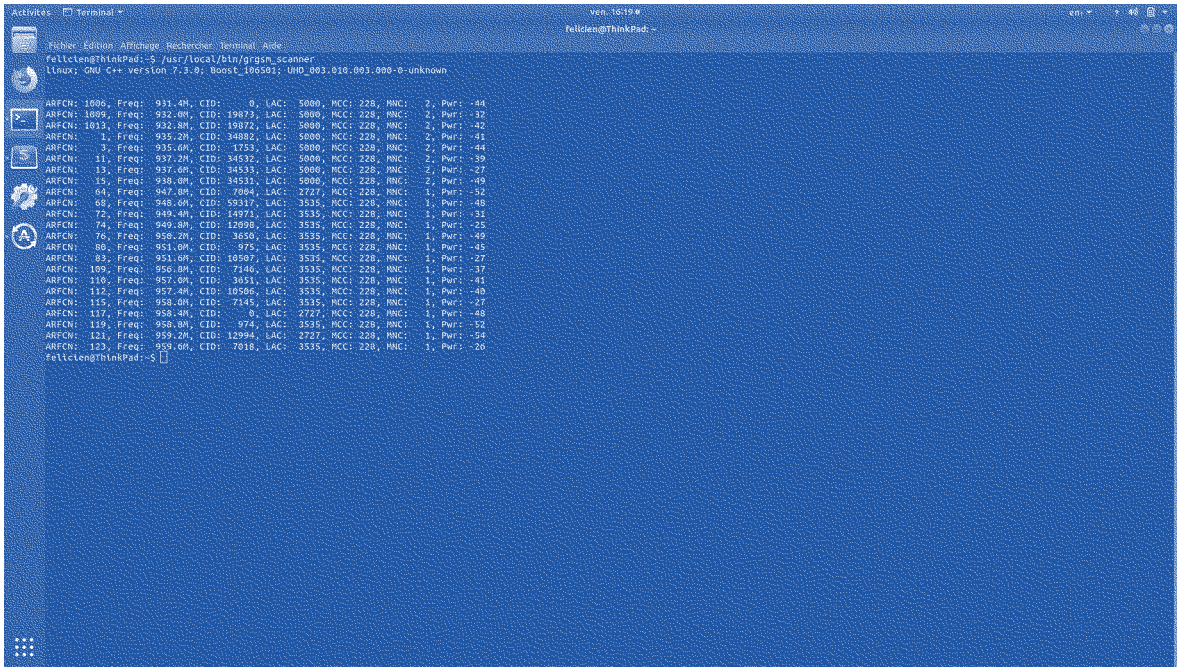


Fig.47. Interface du logiciel Wireshark qui permet d’afficher les packets interceptés ainsi que les IMSIs capturés / Fig.48. REAL: ordinateur portable, Realtek RTL2832U, antenne.



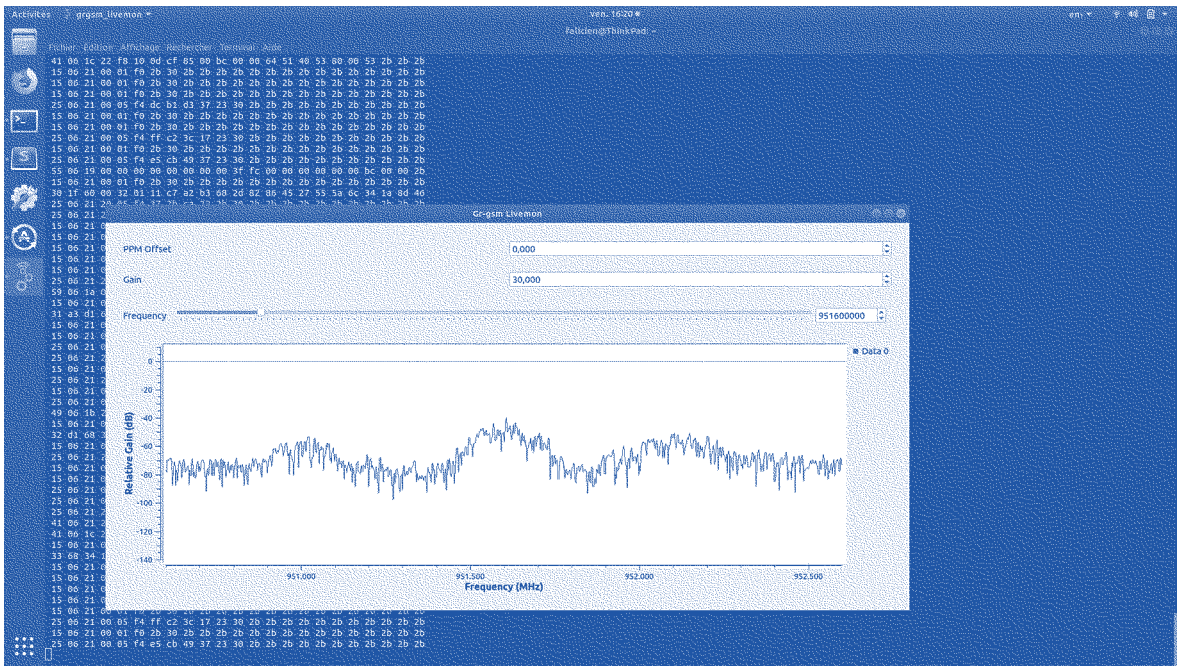


Fig.49. Capture d’écran de l’exécution de grgsm_scanner / Fig.50. Capture d’écran de l’exécution de grgsm_livemon

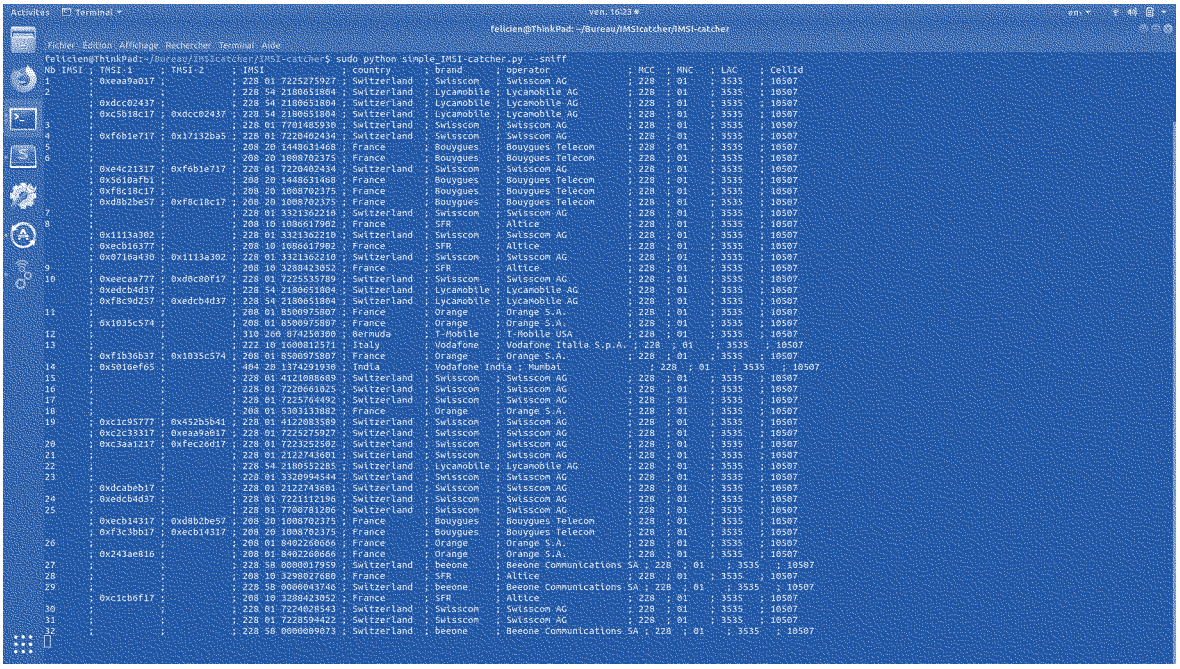


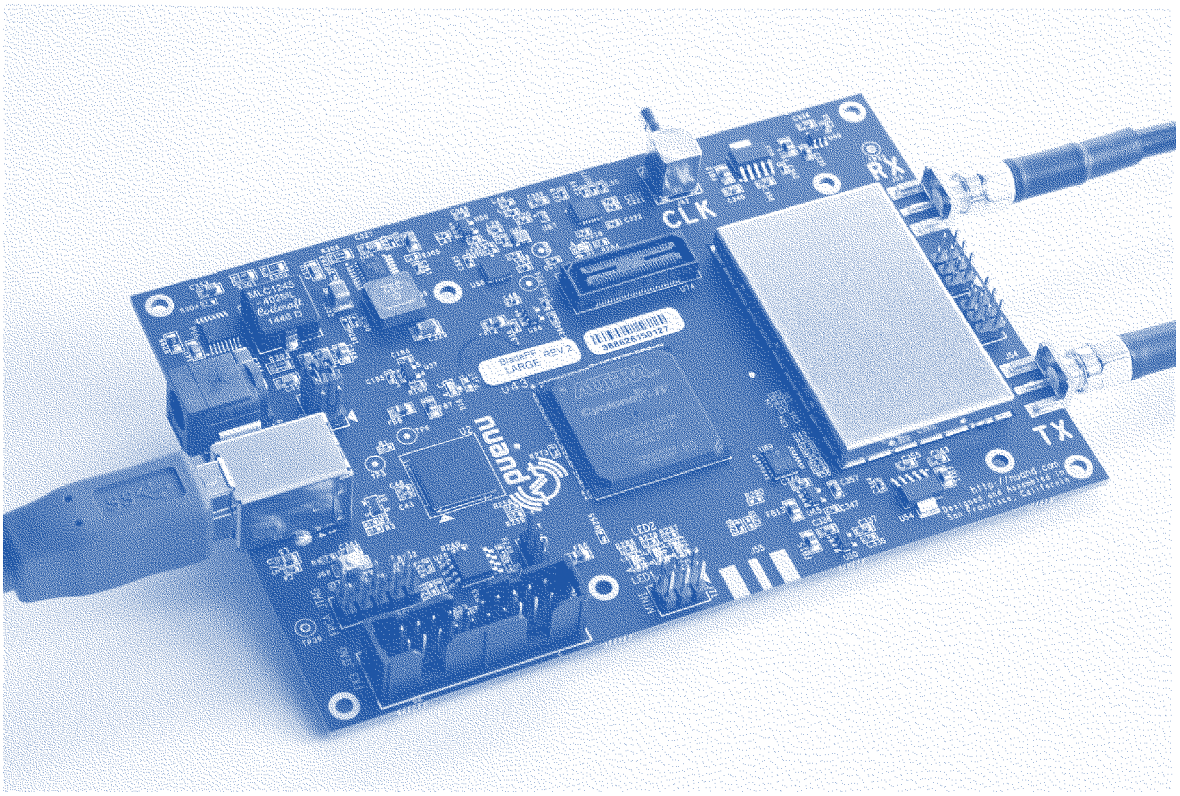
Fig. 51. Capture d’écran de l’exécution du script Python ‘simple_IMSI-catcher.py’ qui affiche les IMSIs en clair.

Un exemple de prototype actif a.k.a. *Blade*

Afin de reproduire un IMSI catcher actif il est nécessaire de configurer une fausse antenne-relais ; ainsi, les téléphones présents aux alentours pensent qu'il s'agit d'une antenne légitime et s'y connectent. Pour pouvoir reconstituer un tel dispositif, j'ai configuré un bladeRF x115 (une carte radio logicielle full duplex, qui est à la fois capable d'émettre et de recevoir, fig. 52) avec YateBTS (une implémentation logicielle open source des protocoles réseaux GSM/GPRS) sur un ordinateur portable sous Ubuntu. YateBTS fournit « Network in a PC » (« NiPC », fig. 53), un *cell site* local qui « effectue toutes les fonctions d'un réseau GSM standard », telles qu'acheminer des appels téléphoniques ou distribuer des messages textuels entre des téléphones locaux. NiPC permet de configurer la fréquence d'émission, mais aussi d'autres critères du réseau tels que : le MCC (Mobile Country Code), le MNC (Mobile Network Code), le LAC (Location Area Code) et le CI (Cell ID).

En effectuant les recherches décrites dans ce chapitre, un *cell site* local (donc non connecté à l'infrastructure GSM existante) a été implémenté (principalement pour des raisons légales). Ainsi, ce réseau était seulement capable d'intercepter l'IMSI des téléphones associés, puis de passer des appels et messages locaux entre ces téléphones (pas de communication sortante). Cependant, en copiant des MCC, MNC, LAC et CI légitimes il est possible d'usurper l'identité d'une antenne relais existante. En redirigeant le trafic au réseau téléphonique existant, sans utiliser d'algorithme de chiffrement (A5/0) entre les téléphones et l'antenne-relais usurpatrice, il est possible d'intercepter des communications.

Toutefois, il existe certaines limites à cette attaque. Tout d'abord, le bladeRF x115 n'a pas une puissance d'émission élevée, seulement les téléphones se trouvant à proximité immédiate peuvent être hameçonnés. Ensuite, il est possible de conduire cette attaque en 2G uniquement, comme l'informaticien et *pentester* Kenneth van Rijsbergen le souligne dans son papier, un smartphone restera préférable ment sur un réseau 3G/4G qui émet faiblement plutôt que de s'associer à un réseau 2G plus puissant (Van Rijsbergen, 2016), par conséquent il est plus facile de cibler des téléphones 2G.



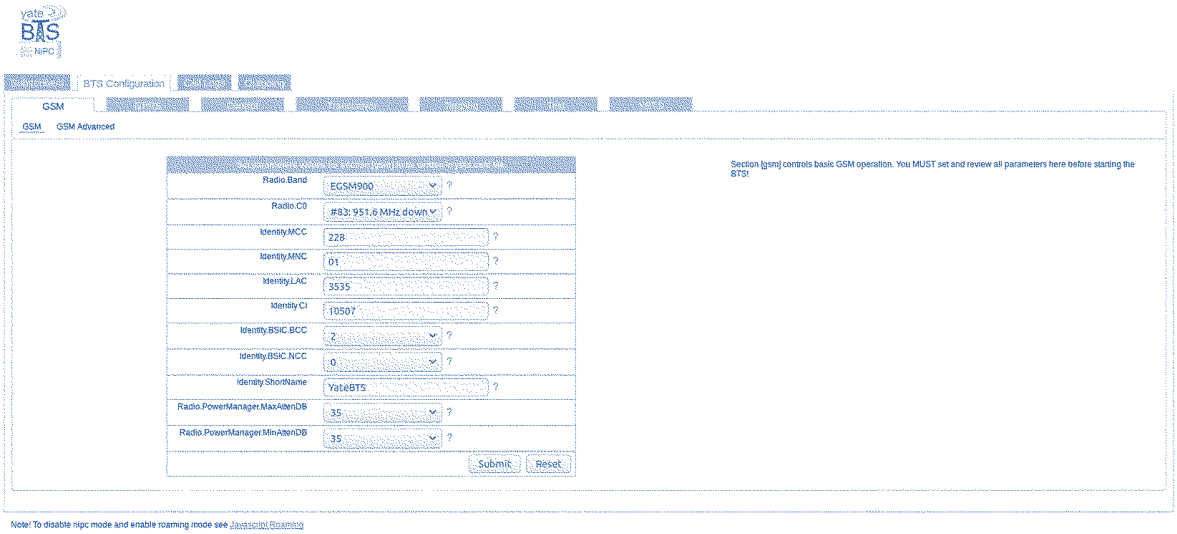


Fig. 52. Nuand BladeRF x115. / Fig. 53. Capture d’écran de l’interface web de Network in a PC

5.2 De la pertinence de reconstituer le présent

Considérant la pertinence de la reconstitution dans les STS et dans les humanités numériques, Sayers utilise ce type de méthodes pour refaire des objets historiques ; pour lui, ces méthodes permettent de produire des connaissances à propos de la « composition », de « l'assemblage », de « l'interface », de « l'échec », de « l'abstraction » de « l'instrumentalisme », et de la « spéculation » (Sayers, 2014). Cette approche est aussi pertinente dans le cas de l'IMSI catcher : bien que n'étant pas un objet historique, c'est un objet confidentiel, et il est possible d'établir un parallèle avec le manque de ressources face à la reconstitution d'un objet historique. Pour un objet historique, des sources documentaires peuvent être manquantes : « même si des médias ne peuvent être entièrement récupérés, le prototypage exerce une pression sur ces changements, et les ouvre à la spéculation » (Sayers, 2015) ; le même principe est valable pour l'IMSI catcher, puisque les sources d'information peuvent être incomplètes, trompeuses ou parfois même non existantes. Ainsi, Sayers ajoute à propos de prototyper le passé (Sayers, 2015) que ces prototypes sont « des rappels tangibles de ce qui a été oublié, ignoré, détruit ou perdu », dans le cas de l'IMSI catcher ce serait plutôt « des prototypes tangibles de ce qui n'est pas encore accessible à tous ». Cette expérimentation par essais et erreurs — « *trial-and-error* » — permet de tester des suppositions à propos de la conception et la production de la technologie étudiée.

Dans « Matters of Composition », Sayers soulève la question des matériaux nécessaires pour reconstruire un artefact historique : « à partir de quels matériaux était-il fait ? ». Pour lui, cette question aborde des problématiques qui touchent non seulement à la composition de l'objet en lui-même, mais aussi à l'approvisionnement des matériaux et des innovations technologiques dans un contexte historique donné. Dans le cas de l'IMSI catcher, je n'ai pas refait le hardware nécessaire à sa production parce que cela requiert des compétences extrêmement avancées en ingénierie électronique et des télécommunications ; j'ai plutôt recherché et assemblé des éléments hardware disponibles en vente libre — « off-the-shelf » — tels que des ordinateurs portables, des cartes radio et des antennes. Un point intéressant toutefois, est la disponibilité sur le marché public et l'origine d'un téléphone portable à 30 $, d'un *dongle* TV numériques à 10 $ et d'une carte SDR dédiée large bande full duplex à 700 $. En effet, pour les moins coûteux, n'importe qui peut les commander sur eBay ou des sites web chinois dans le sens où ceux-ci ne sont pas prévus pour l'usage que j'en ai fait. Pour le dernier, c'est légèrement différent puisqu'il est obligatoire de déclarer dans quel pays et pour quelles raisons il va être utilisé — dans le cas présent, situer la recherche dans un contexte académique semble avoir facilité le processus de commande. Cela soulève la question de la légalité de la détention de tels dispositifs : les objets susmentionnés ne sont pas illégaux en soit, mais leur utilisation comme des IMSI catchers l'est.

Dans « Matters of Assembly », Sayers pose la question suivante : « à travers quels processus a-t-il été fabriqué ? ». Pour lui, « un intérêt dans le processus est souvent un intérêt qui ne peut pas être recouvré du matériel historique à disposition » ; dans notre cas c'est un intérêt qui n'est pas disponible de sources publiques. En effet, les essais pour réassembler un IMSI catcher étaient d'abord basés sur des éléments picturaux, comme des photographies d'IMSI catchers existants dans des catalogues ayant fait l'objet de fuites (dans lesquels il est possible de trouver une multitude de formes allant de l'objet de poche à des boîtes noires faisant la taille d'une armoire électrique), ou sur des sites de vente en ligne comme Alibaba.com. En dehors des différentes formes de ces dispositifs et de la nature de certains de leurs composants, ces images n'informent guère sur la façon dont ils opèrent. Comme il a été dit plus tôt, la source d'information principale est à trouver auprès des communautés *open source* qui fournissent une documentation abondante pour la reconstitution d'IMSI catchers « afin de mieux comprendre l'infrastructure GSM », ou pour bâtir des sites femto ou picocellulaires dans des zones non couvertes. Dans ce sens, essayer de mieux comprendre les processus (ou les faiblesses) sur lesquels l'IMSI catcher repose est une manière de questionner sa nature et de discuter son caractère confidentiel ; si l'on paraphrase Sayers : « l'IMSI catcher fonctionne-t-il comme on le pense ? Fonctionne-t-il seulement ? ». Cela soulève la question des représentations (souvent erronées) des technologies confidentielles et de la façon dont elles opèrent réellement ; refaire plusieurs versions d'IMSI catchers a permis de mieux comprendre ces processus de fonctionnement et d'exposer les limites potentielles des dispositifs qui en réalité ne fonctionnent pas comme le grand public le pense. Enfin, dans l'approche historique de Sayers « ces questions encadrent les technologies comme des processus, non comme des produits gelés dans le temps » ; ce qui est aussi pertinent dans le cas de l'IMSI catchers puisque c'est un objet contemporain en constante évolution.

Dans « Matters of Interface » Sayers discute à travers quels types d'interactions l'objet a été réalisé, utilisé ou comment il a circulé. Dans le cas de l'IMSI catcher « l'interface » est très peu documentée voire pas du tout, étant donnée la nature secrète de l'objet, dont l'usage est connu, mais jamais révélé en présence du public. Toutefois, il fait certaines apparitions dans des budgets publics (ce qui renseigne le nom des entreprises qui le commercialisent et leur prix), dans des textes de lois et son utilisation a été rapportée dans différents contexte — d'espionnage industriel en Inde par exemple (Parks, 2016). Ceci soulève certaines questions telles que la potentielle automatisation de ces dispositifs, le niveau technique requis pour les utiliser ou s'ils ont seulement besoin d'un opérateur pour fonctionner (on peut fortement supposer que oui). Si la reconstitution permet d'apprendre au sujet des « interfaces » dans les communautés *open source* et s'il est possible d'automatiser le fonctionnement avec quelques scripts ; il est quasiment impossible de répondre à ces questions du point de vue des services

gouvernementaux qui en font l'usage. En effet, il n'est pas possible dans notre cas d'affirmer que les IMSI catchers utilisés par les services de renseignement et les forces de l'ordre reposent sur les mêmes configurations matérielles et logicielles. Par conséquent, il est impossible de tirer des conclusions précises à propos de leur utilisation, mais cela ouvre à la spéculation, ce qui n'aide pas dans l'idée de lever le voile sur l'aspect confidentiel de la technologie. Cela montre les limites du processus de reconstitution pour répondre à certaines questions.

« Matters of Failure » aborde la question du succès de l'objet. Il est quasiment impossible d'évaluer le succès de l'IMSI catcher à partir de la documentation disponible. S'il est déjà difficile de trouver des informations pertinentes sur des IMSI catchers opérationnels, les sources d'informations à propos d'IMSI catchers abandonnés n'existent pas. Même si la reconstitution n'a pas donné lieu à un IMSI catcher qui ne fonctionnait pas, le processus a suscité une approche d'erreurs et d'essais et a permis de faire la lumière sur une multiplicité d'objets fonctionnant de différentes façons sous le même nom, ce qui implique que différentes versions co-existent probablement avec leur propre efficacité ou « succès » au sein des services qui les utilisent.

Dans « Matters of Abstraction » Sayers pose la question : « À travers quel média a-t-il été présenté et comment ? » ce qui dans notre cas réfère à la question des sources et de la documentation des dispositifs. Comme il l'a été dit plus tôt, tandis que les catalogues donnent une représentation visuelle et parfois les dimensions des dispositifs, les communautés *open source* donnent des logiciels (sous la forme de code source) pour les reconstituer. C'est l'articulation de ces différentes sources qui permettent la reconstitution du dispositif et qui permettent d'explorer sa nature et ses principes de fonctionnement. Comme Sayers l'écrit, « chacun de ces arguments résume plusieurs dimensions, positions et perspectives, traduisant la relation entre-elles en quelque chose de communicable, d'interprétable et d'archivable. La reconstitution d'un dispositif est hantée par des relations abstraites, nous rappelant que nous ne pouvons pas totalement récupérer les processus incarnés tout en nous donnant un sens granulaire de ce que ces processus ont pu entraîner ». Ainsi, il est possible de montrer ce à quoi un IMSI catcher ressemble et comment il fonctionne si l'on prend soin d'articuler les différentes sources d'informations que nous avons à disposition.

« Matters of Instrumentalism » soulève la question de la documentation du processus de reconstitution et des objets reconstitués. Dans le cas singulier de l'IMSI catcher, le but de la recherche n'est pas d'écrire un manuel qui indiquerait comment produire le plus efficace, mais plutôt d'explorer sa nature et son caractère confidentiel, puis, d'accumuler assez de matériel pour poursuivre les différentes étapes de la recherche. Puisque j'approche cette recherche d'une perspective de

design basée sur la pratique, certains des résultats de ces reconstitutions ont été présentés dans des expositions et au cours de performances comme nous le verrons plus loin.

Le dernier point que Sayers aborde à propos de la pertinence de la reconstitution est « Matters of Speculation ». Dans l'approche historique, cela concerne ce que l'on ne connait pas, ce qui n'est pas à disposition. Ces deux questions sont évidemment au cœur de la recherche lorsqu'on s'intéresse à une technologie confidentielle. Dans un souci historique, lorsqu'aucune documentation n'est disponible, une partie de la reconstitution repose sur de la spéculation. Ainsi, les chercheurs « construisent et testent une variété de possibilités, tout en les comparant avec ce qui était disponible ou populaire à l'époque, et ce faisant déterminent ce qui est réalisable pour la distribution. ». C'est ce que j'ai en partie fait en recréant et en testant différentes itérations d'IMSI catchers ; de plus, je suis allé au-delà de cette étape en conceptualisant des prototypes de contre-surveillance potentiels que nous aborderons dans le chapitre suivant.

5.3 Mythes et spéculation

Il existe un aspect spéculatif inhérent aux technologies confidentielles. Comme cela a été dit plus tôt, la spéculation est nécessaire lorsque nous n'avons pas toutes les ressources à disposition, ce qui n'est pas connu doit être spéculé. Mais traiter d'une technologie aussi confidentielle ouvre un autre espace de spéculation : l'espace de ce qui est à venir (des futurs spéculatifs) ou ce qui aurait pu être (des présents alternatifs), ce qui constitue probablement le point le plus important dans le processus de recherche d'une perspective de design fiction.

En ce sens, l'idée derrière la démystification de l'objet IMSI catcher à l'aide d'une approche de rétro-ingénierie n'est pas de remplacer une représentation par une autre, puisque cela amènerait d'autres préoccupations et mythes. Ce n'est pas une fin en soi, mais cela devrait plutôt être vu comme une étape pour ouvrir un nouvel espace dédié à la spéculation. Ainsi, en ce basant sur d'autres formes existantes de l'IMSI catcher et sur des signaux faibles (par exemple des dispositifs embarqués sur des drones, des prototypes *wearable*), il est possible d'inférer des dispositifs « qui restent à venir ».

Si cette approche de design spéculatif permet de s'affranchir des contraintes technologiques et techniques, il est néanmoins important de garder à l'esprit les réalités des objets existants. La reconstitution d'un ou de plusieurs IMSI catchers établit une base de connaissances qui permet de mieux comprendre la technologie et constitue le point de départ pour « élaborer la spéculation » (Auger, 2013). En effet, comme l'argumente Auger, baser des visions sur des « trajectoires logiques » ou « les règles de la vraie vie » permet « d'élaborer la spéculation dans

quelque chose de plus poignant, basé sur des itérations logiques d'une technologie émergente et taillé en fonction des exigences complexes et subtiles d'une audience identifiée ». Dans le cas de l'IMSI catcher, cela permet de surmonter sa nature confidentielle dans le but d'obtenir des « présents alternatifs et des futurs spéculatifs » (Auger, 2013). Ainsi, l'élaboration de scénarios spéculatifs soulève des points de tensions pour débuter une réflexion plus globale à propos de la légitimité et l'éthique dans le déploiement de tels systèmes de surveillance. Ensuite, concevoir des itérations à propos de futurs spéculatifs ou de présents alternatifs de l'IMSI catcher donne la possibilité de réfléchir aux conséquences de son utilisation présente et de développer une éventuelle critique.

5.4 Vers la constitution d'une boîte à outils

Dans ce chapitre nous avons vu qu'il était possible d'aborder le caractère confidentiel d'une technologie en se basant sur un processus pratique de reconstitution. La reconstitution de trois différentes versions d'IMSI catchers a permis de faire face au manque de documentation. En utilisant du hardware en ventre libre et du software *open source*, il est possible de recréer des dispositifs similaires afin d'explorer et d'apprendre sur son fonctionnement et l'environnement sur lequel il repose. L'utilisation de méthodes de reconstitution permet de se réapproprier la technologie, mais permet aussi d'exposer ses limites et ses dépendances vis-à-vis de son environnement. De cette manière, le processus de refaire les incarnations d'une telle technologie permet de discuter son caractère confidentiel. Comme nous avons pu le voir, l'IMSI catcher ne fonctionne pas comme le grand public pourrait le penser et montre certaines limites dans sa zone d'utilisation et dans le type de téléphones concernés par ce genre d'attaques.

En comparant avec l'approche historique de Sayers, nous avons aussi discuté la pertinence de la reconstitution lorsque l'on traite d'un objet contemporain. Cette approche constituée d'essais et d'erreurs permet de faire face au caractère confidentiel d'une technologie actuelle et au manque de ressource, cela permet de répondre à un certain nombre de questions sur son fonctionnement même ou sur la façon dont elle est supposée fonctionner.

Toutefois, il y a des limites évidentes à une telle méthodologie. En effet, le matériel utilisé ici ne correspond pas aux spécifications techniques de celui utilisé par les agences de renseignement gouvernementales : les moyens utilisés pour mener cette recherche ne sont pas dédiés à la surveillance, il s'agit plutôt ici d'un détournement de leur usage premier. Ainsi, il est seulement possible de spéculer à propos des fonctionnalités exactes des dispositifs détenus par les agences de renseignement. Le processus entier est un genre d'approximation qui dévoile seulement une partie du mystère qui entoure de tels objets de la surveillance.

Finalement, les résultats présentés ici constituent une boîte à outils pour élargir la recherche dans le champ de la surveillance, en ce sens que nous pourrions probablement utiliser la même méthodologie pour d'autres objets de la surveillance afin d'explorer leur vraie nature et leurs effets. C'est aussi une boîte à outils — constituée d'éléments logiciels (différents programmes d'acquisition et de traitement des données du réseau téléphonique mobile) et matériels (antennes et cartes radio différentes selon l'objectif visé) — pour examiner d'autres caractéristiques de l'objet comme son propre processus de concrétisation et ses effets sur son milieu associé (Simondon, 1958) ; en ce sens, c'est une base de spéculation pour imaginer les lignées techniques des dispositifs futurs.

5.5 Produire à partir de la reconstitution : 900 MHz

Les différentes itérations d'IMSI catchers reconstitués constituent des objets intermédiaires (Vinck, 2009). Dans la recherche, ceux-ci sont des jalons qui permettent (1) de comprendre le fonctionnement même de l'objet et de ses différentes composantes, (2) de comprendre ses modes d'interaction avec son environnement (le réseau et ses usagers), (3) une utilisation pour d'autres types de productions. Une des productions directement issue de la reconstitution est *900 MHz* (pp.120-134).

9*00 MHz* est une performance audiovisuelle qui tente de rendre compte de l'activité du réseau téléphonique mobile. Elle tient son nom de « 900 MHz » qui est la bande de fréquences utilisée pour les communications téléphoniques mobiles GSM. Les IMSI catchers passifs présentés plus haut ont permis d'acquérir des données en temps réel du réseau, puis elles ont été interprétées en image et en son à l'aide de techniques de design génératif et paramétrique ; j'ai pour cela collaboré avec le designer sonore Yann Longchamp, la *sonification* des données vient ainsi compléter les visuels génératif et permet d'obtenir une expérience audiovisuelle complète qui rend l'activité du réseau plus saisissable. La performance s'ouvre sur une série d'antennes relais, seule partie visible et identifiable de l'infrastructure téléphonique mobile. Le traitement des images évoque la représentation fréquentielle d'un signal radio. La seconde partie dessine cette infrastructure en écoutant tour à tour les différentes antennes relais environnantes. Cette écoute permet d'obtenir des informations sur chacune des cellules du réseau, leur interprétation visuelle et sonore révèle un paysage électromagnétique dissimulé et habituellement imperceptible. Enfin, la dernière phase se concentre sur des antennes relais spécifiques et révèle les IMSIs des téléphones mobiles qui s'y connectent. Les données interceptées permettent de déterminer la provenance et l'opérateur des téléphones, ce qui se rapproche de l'usage de l'IMSI catcher fait par les forces de l'ordre.

La performance a été jouée à Genève à l'occasion de la Nuit des musées 2019 (fig. 54), à Mourmansk pour le festival Inversia 2019 et Saint-Pétersbourg pour le Cyfest 2019 (fig. 55 et 56). Elle a aussi été présentée sous forme d'installation à la Maison des arts électroniques à Bâle lors de l'exposition Swiss Media Art 2020. Ces différentes interventions, en utilisant la reconstitution permettent une forme d'appropriation de la technologie et un détournement de celle-ci à des fins tout à fait différentes de ce pour quoi elle a été conçue. Si je n'ai pas réalisé d'enquête spécifique sur l'appropriation du dispositif, les échanges avec les visiteurs, avant et après les performances sont tout de même pertinents pour saisir différents enjeux liés à la perception de l'IMSI catcher.

Une des questions qui m'a été adressée à la sortie de la performance au MEG de la part d'un spectateur a été : « et la 5G, vous en pensez quoi ? ». Cette simple évocation de la 5G fait écho à l'« aliénation » décrite par Simondon à propos de la méconnaissance des objets techniques (Simondon, 1958, p.9-10) ; en effet, le spectateur après avoir vu une partie des capacités de l'IMSI catcher sur la 2G les a immédiatement associées à la génération actuellement en développement alors que l'IMSI catcher ne fonctionne pas sur le protocole utilisé pour la 5G (rappelons qu'il exploite des failles du protocole GSM uniquement, utilisé en 2G). Cette interrogation illustre un décalage entre la perception du phénomène et le phénomène lui même, symptomatique d'« une méconnaissance de la machine » pour reprendre les mots du philosophe des techniques.

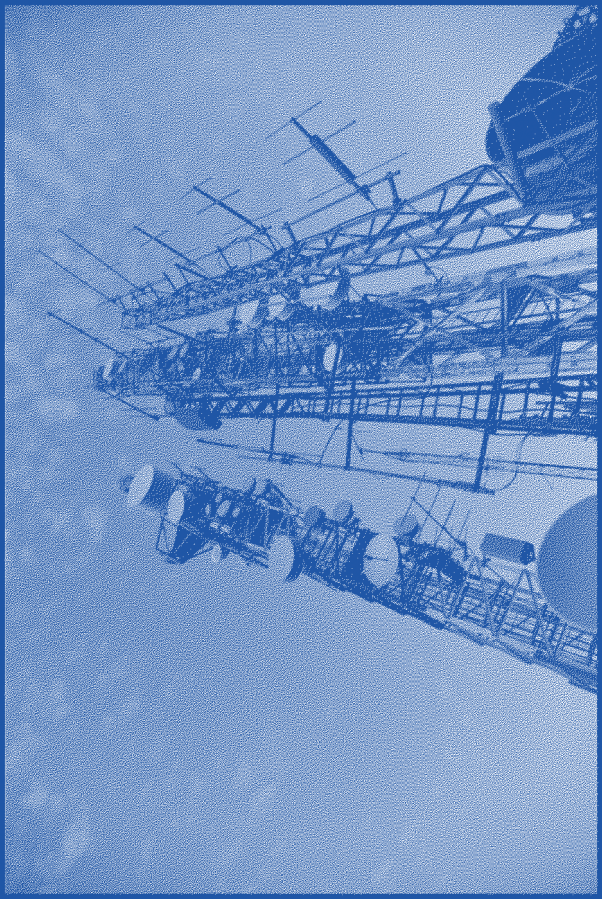
D'autres réactions ont permis de cerner l'inquiétude du public vis-à-vis du dispositif : « Ah mais si vous arrivez à faire ça, qu'est-ce qu'*ils* doivent pouvoir faire », s'interloquait une spectatrice. Là encore, la performance en elle même suscite des imaginaires plus vastes et plus inquiétants encore sur les capacités d'organisations ici non précisées et décrites par ce "*ils*" impersonnel et renvoyant à une puissance difficile à qualifier. Toutefois, malgré cette inquiétude on peut supposer que la plupart du public n'a pas modifié ses habitudes au sortir de la performance. De la même façon en Russie, alors que j'étais moi-même pris dans des inquiétudes liées au transport de matériel potentiellement suspect ou illégal ou aux conséquences de l'écoute du réseau téléphonique dans un pays autour duquel on développe un imaginaire sécuritaire et policier dur, j'ai été surpris de trouver un public plus fasciné par la prouesse technique et impacté par la transformation esthétique visuelle et sonore des données interceptées que par le phénomène de surveillance en question et les conséquences socio-politiques potentielles .

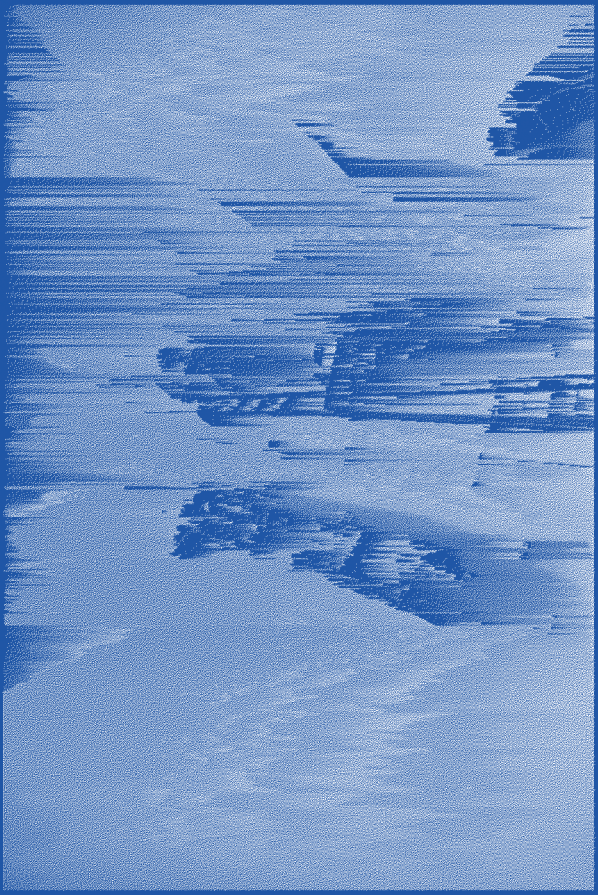
Malgré les discours médiatiques et l'effort que je produis dans la mise en forme et la monstration d'un phénomène techno-politique réel et inquiétant, l'effet de prise de conscience ou la volonté établir un débat recherchés ne sont là pas tout à fait atteints. Aussi, on se retrouve face au « paradoxe de la vie privée » : on a

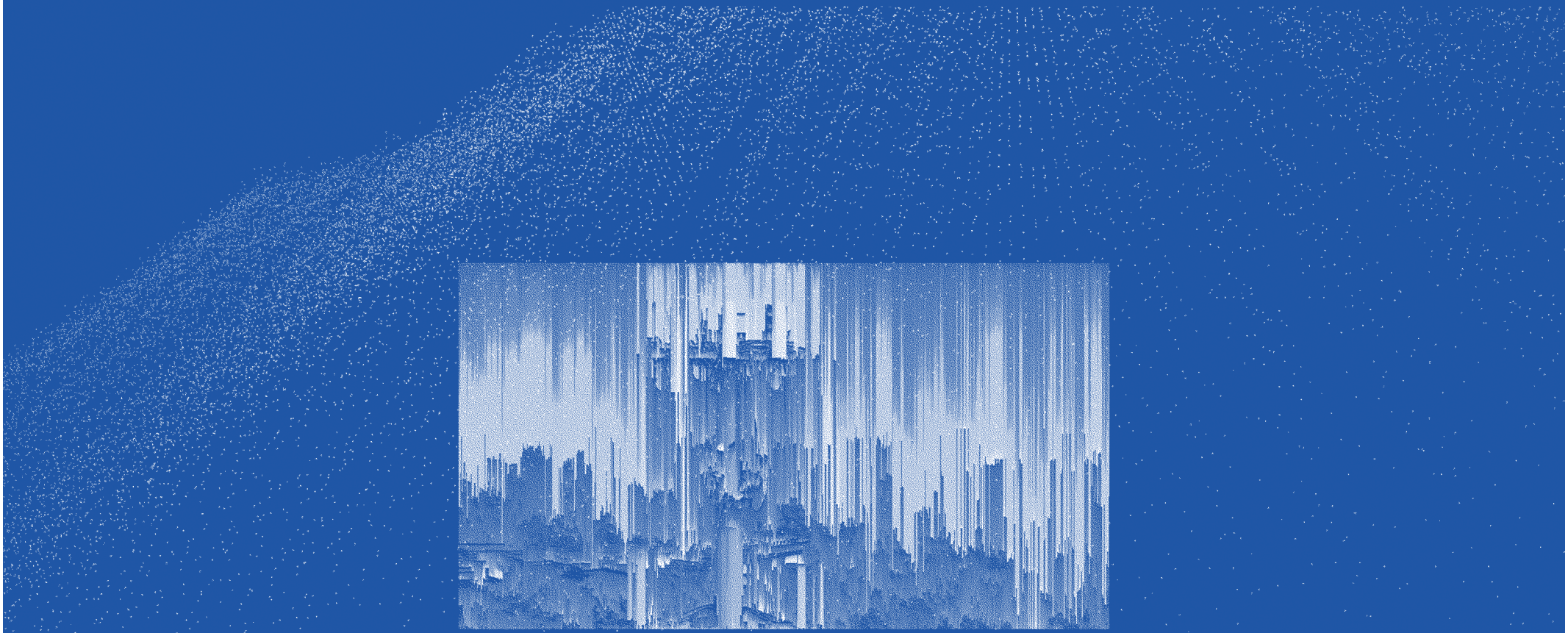
beau être au courant, ça n'est pas pour autant qu'on change drastiquement nos pratiques. Ce paradoxe est notamment identifié par la sociologue Susan Barnes à propos des réseaux sociaux (Barnes, 2006), dans lequel elle décrit comment les adolescents donnent leurs données personnelles pour profiter des réseaux sociaux mais s'étonnent ensuite que leurs parents lisent leur *feed* ; elle expose ainsi des frontières toujours plus poreuses entre vie privée et vie public. Ce paradoxe ne s'applique pas uniquement aux adolescents mais bien à tous les individus dans leur relation à la technologie : tiraillés entre le souci du respect de leur vie privée et le désir de jouir de l'avantage des nouvelles technologie. Mais voyons maintenant dans le chapitre suivant, comment la reconstitution permet la production d'autres formes d'objets et de réflexions.

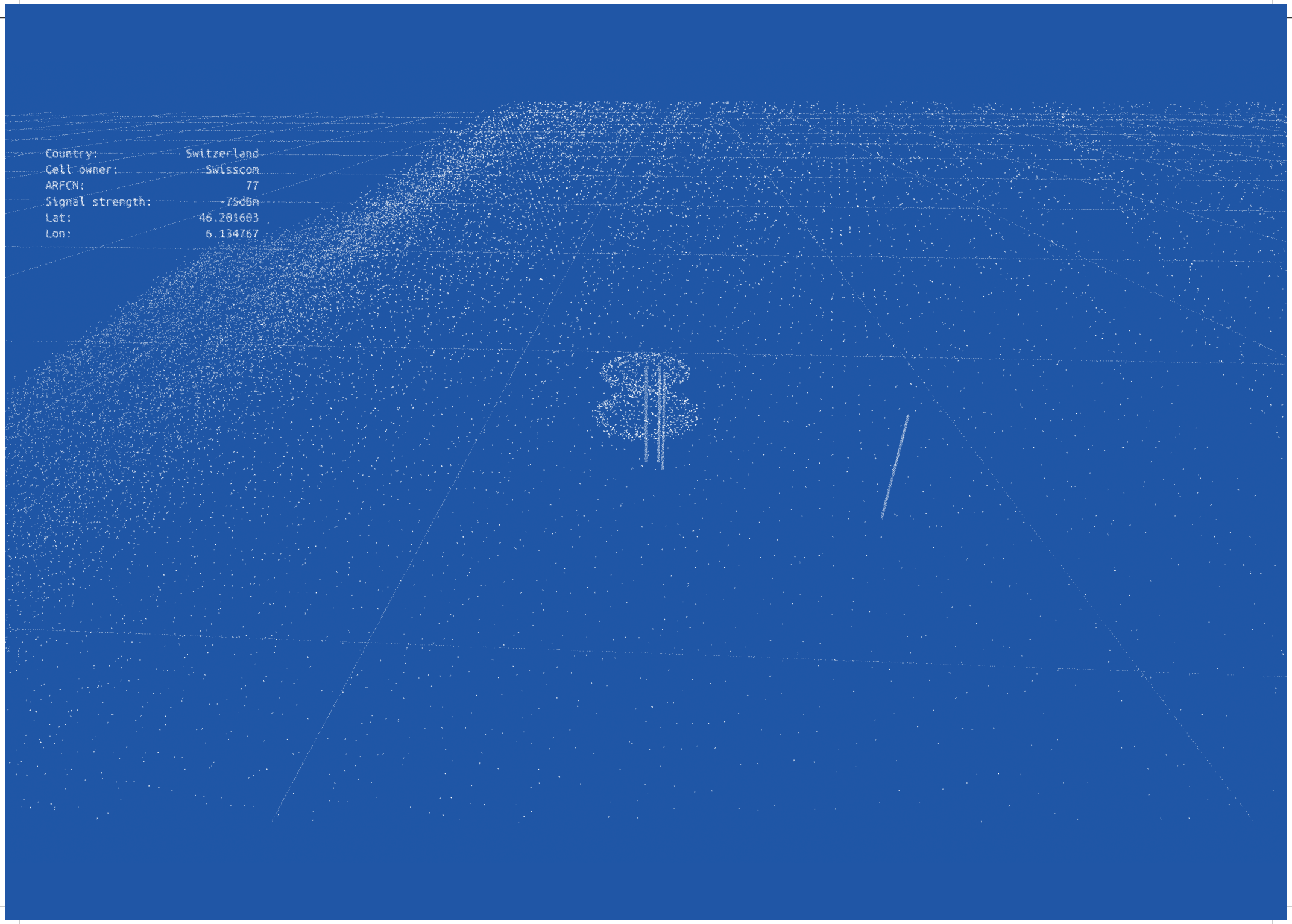
Fig. 54. Félicien Goguey, Yann Longchamp. *900 MHz*. Live au MEG, Genève. 18.05.2019.
Photo : Nicolas Nova.

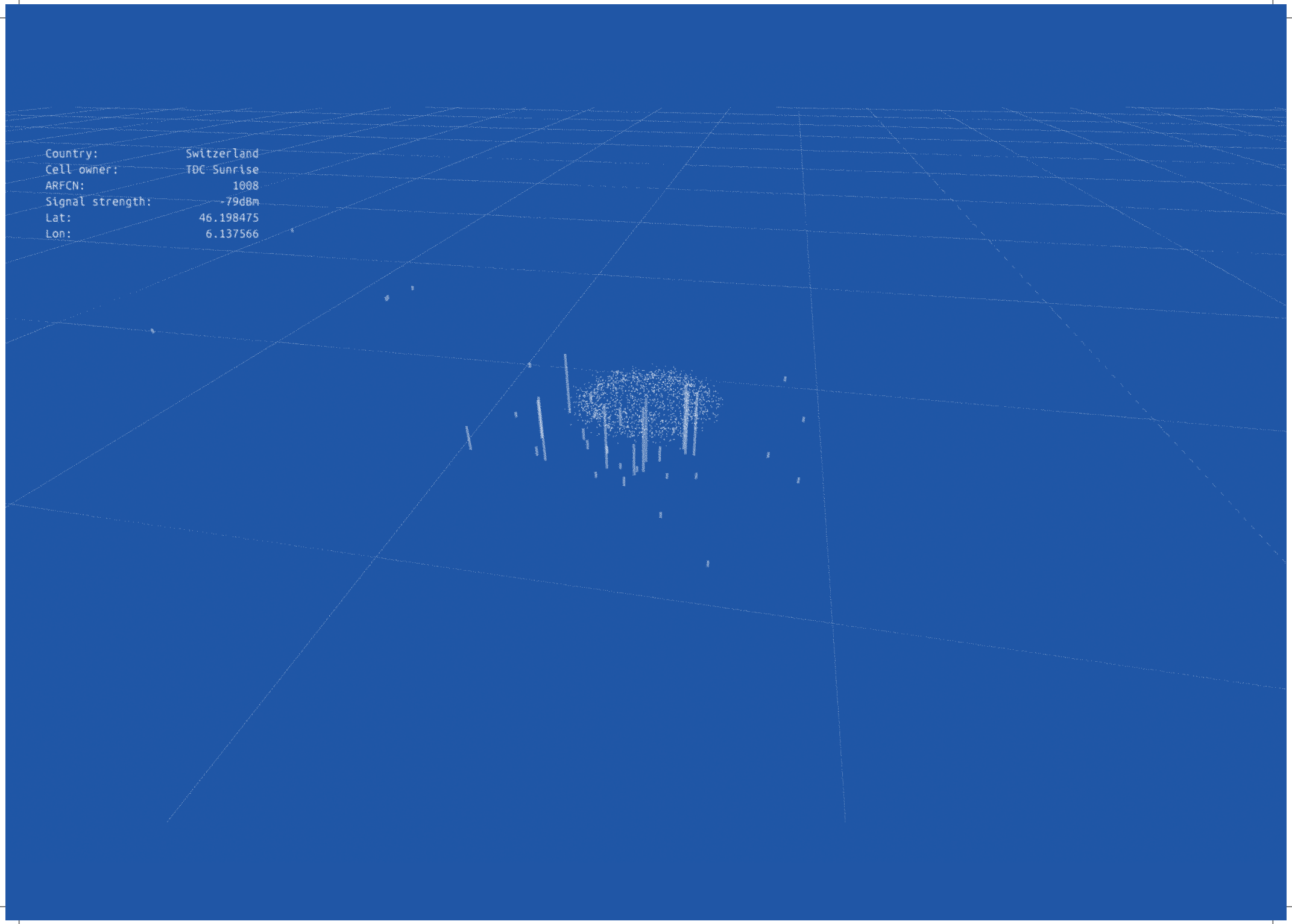
Fig. 55. Félicien Goguey. Capture de données GSM. Saint-Pétersbourg. 21.11.2019. /
Fig. 56. Félicien Goguey, Yann Longchamp. *900 MHz*. Live au Cyfest 12, Saint-Pétersbourg. 22.11.2019. Photo : Anton Khlabov.

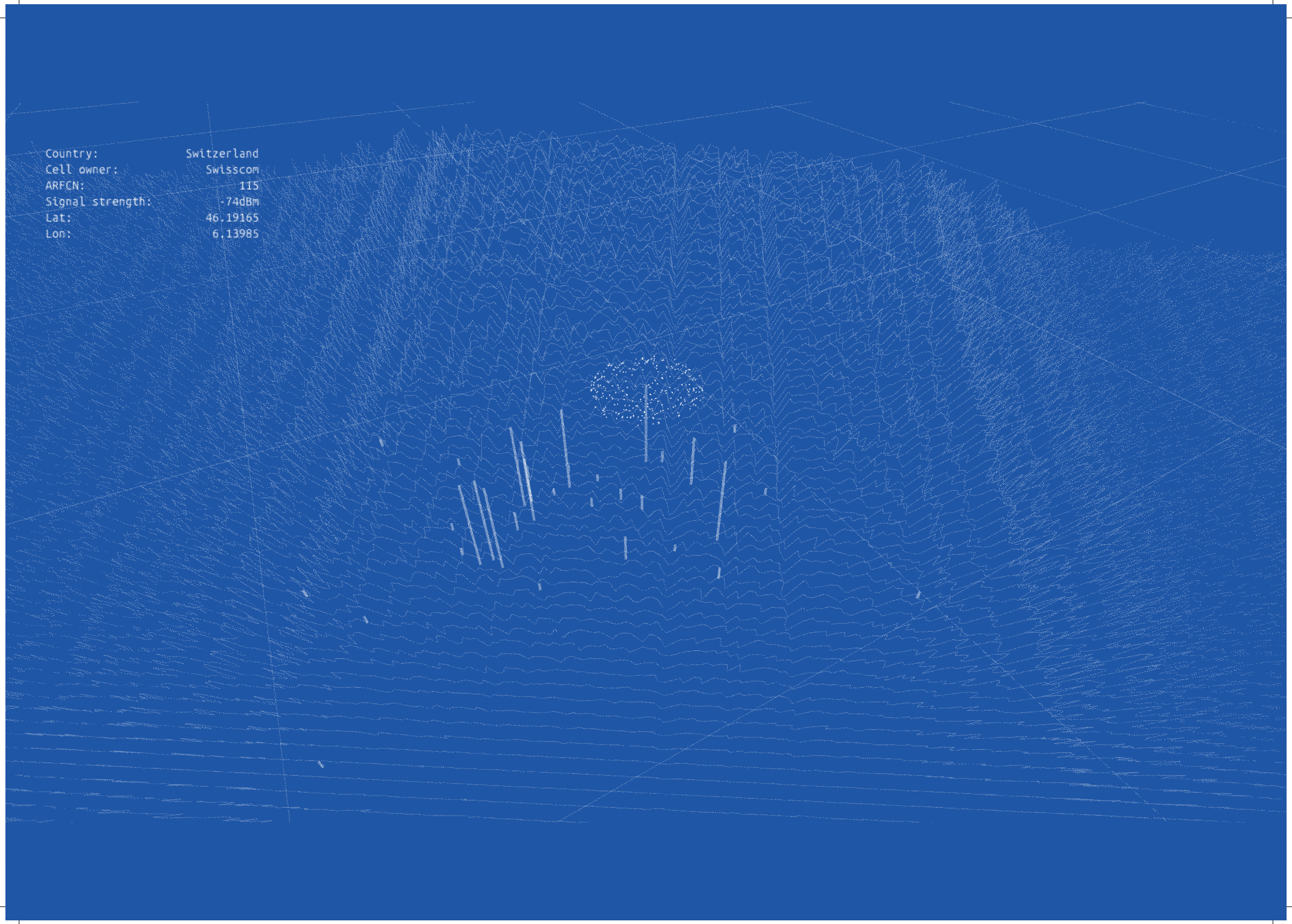


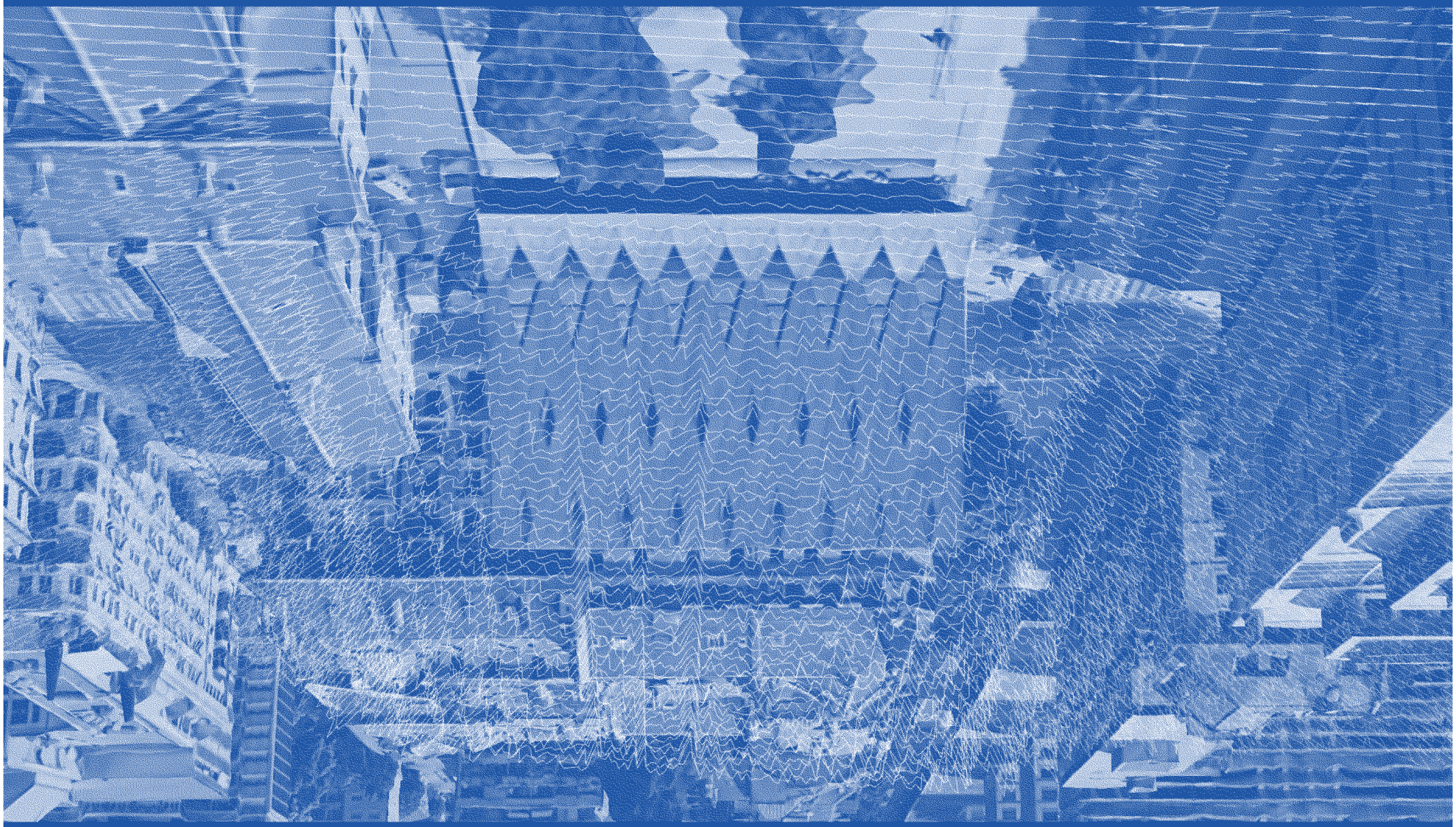





Country: Switzerland
Cell owner: Swisscom
ARFCN: 77
Signal strength: -75dBm
Lat: 46.201603
Lon: 6.134767


Country: Switzerland
Cell owner: TDC Sunrise
ARFCN: 1008
Signal strength: -79dBm
Lat: 46.198475
Lon: 6.137566


Country: Switzerland
Cell owner: Swisscom
ARFCN: 115
Signal strength: -74dBm
Lat: 46.19165
Lon: 6.13985



```
Listening to 959.6 MHz.

310 260 1864XXXXX - Bermuda - T-Mobile - T-Mobile USA
260 03 29998XXXXX - Poland - Orange - Polska Telefonia Komrkowa Centertel Sp. z o.o.
228 01 72250XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 72237XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 72283XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 59301XXXXX - Switzerland - Swisscom - Swisscom AG
```

```
Listening to 931.8 MHz.

228 02 15032XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13046XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15047XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13326XXXXX - Switzerland - Sunrise - Sunrise Communications AG
605 03 09074XXXXX - Tunisia - OOREDOO TN - ooredoo Tunisiana
228 02 13326XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 16121XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13326XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15034XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15031XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 35481XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13326XXXXX - Switzerland - Sunrise - Sunrise Communications AG
208 10 75932XXXXX - France - SFR - Altice
228 02 15031XXXXX - Switzerland - Sunrise - Sunrise Communications AG
605 03 09074XXXXX - Tunisia - OOREDOO TN - ooredoo Tunisiana
228 02 43563XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15046XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15045XXXXX - Switzerland - Sunrise - Sunrise Communications AG
262 01 48440XXXXX - Germany - Telekom - Telekom Deutschland GmbH
228 02 15046XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 43564XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 35469XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13036XXXXX - Switzerland - Sunrise - Sunrise Communications AG
602 02 21895XXXXX - Egypt - Vodafone - Vodafone Egypt
228 02 15036XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15048XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13152XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15047XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15048XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13031XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15045XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13148XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13151XXXXX - Switzerland - Sunrise - Sunrise Communications AG
```

Listening to 957.8 MHz.

228 01 47006XXXXX - Switzerland - Swisscom - Swisscom AG
260 03 23374XXXXX - Poland - Orange - Polska Telefonia Komrkowa Centertel Sp. z o.o.
228 01 47006XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 72229XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 44202XXXXX - Switzerland - Swisscom - Swisscom AG
208 20 08514XXXXX - France - Bouygues - Bouygues Telecom
228 01 72229XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 47006XXXXX - Switzerland - Swisscom - Swisscom AG

Listening to 937.6 MHz.

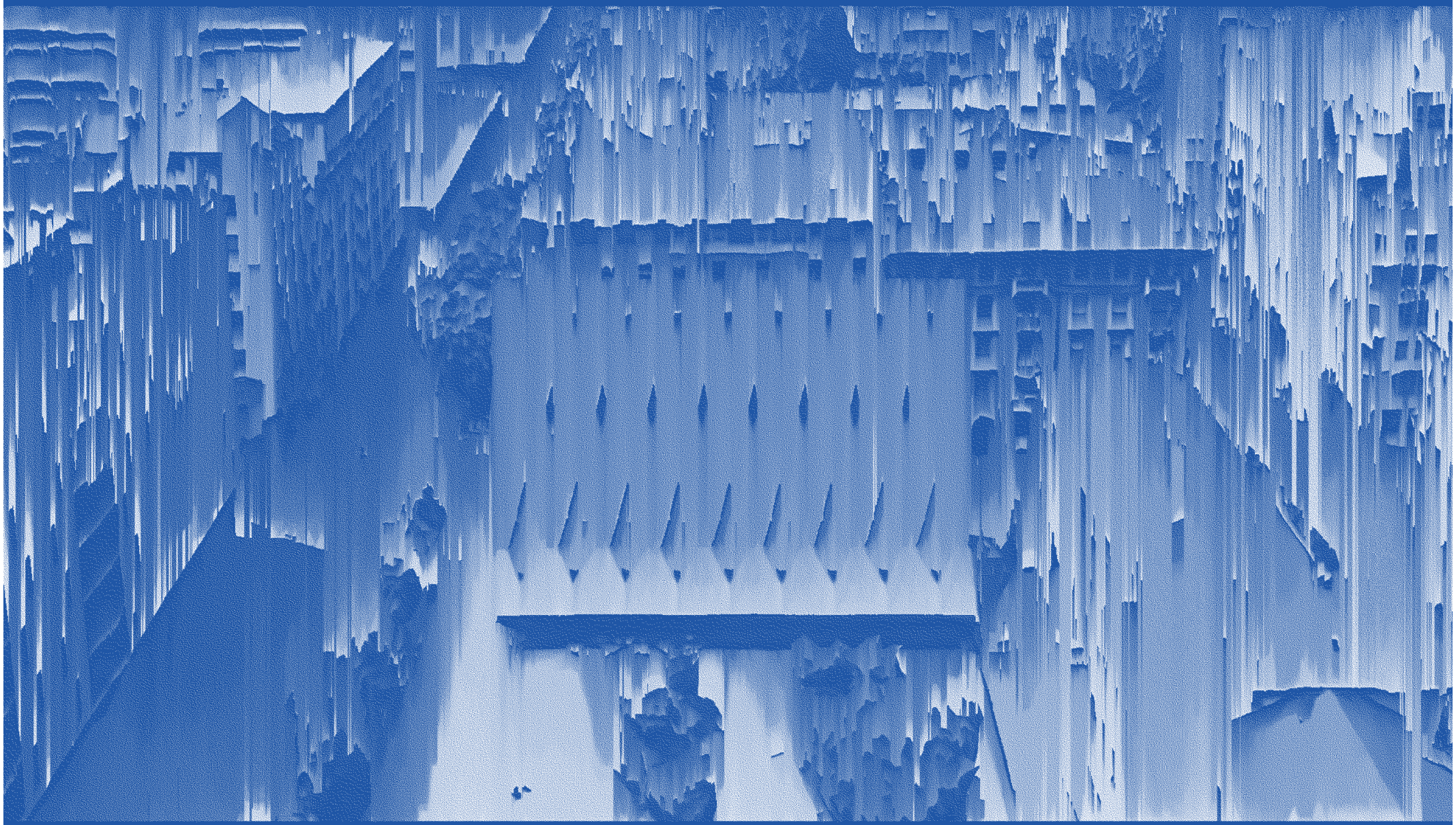
228 02 15182XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13147XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13140XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15024XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13150XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15033XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13037XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13146XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13140XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13070XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13152XXXXX - Switzerland - Sunrise - Sunrise Communications AG
208 01 68026XXXXX - France - Orange - Orange S.A.
228 02 13150XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13070XXXXX - Switzerland - Sunrise - Sunrise Communications AG

Listening to 957.8 MHz.

228 01 47006XXXXX - Switzerland - Swisscom - Swisscom AG
260 03 23374XXXXX - Poland - Orange - Polska Telefonia Komrkowa Centertel Sp. z o.o.
228 01 47006XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 72229XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 44202XXXXX - Switzerland - Swisscom - Swisscom AG
208 20 08514XXXXX - France - Bouygues - Bouygues Telecom
228 01 72229XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 47006XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 72234XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 59301XXXXX - Switzerland - Swisscom - Swisscom AG
228 01 72254XXXXX - Switzerland - Swisscom - Swisscom AG
228 54 21801XXXXX - Switzerland - Lycamobile - Lycamobile AG
228 54 21811XXXXX - Switzerland - Lycamobile - Lycamobile AG
228 54 21804XXXXX - Switzerland - Lycamobile - Lycamobile AG

Listening to 937.6 MHz.

228 02 13146XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13070XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15037XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 03301XXXXX - Switzerland - Sunrise - Sunrise Communications AG
206 01 88807XXXXX - Belgium - Proximus - Belgacom Mobile
228 02 15046XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15044XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15041XXXXX - Switzerland - Sunrise - Sunrise Communications AG
206 01 88807XXXXX - Belgium - Proximus - Belgacom Mobile
228 02 15044XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15041XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 35432XXXXX - Switzerland - Sunrise - Sunrise Communications AG
206 01 88807XXXXX - Belgium - Proximus - Belgacom Mobile
228 02 13036XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 35432XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15047XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15031XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15026XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15047XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15046XXXXX - Switzerland - Sunrise - Sunrise Communications AG
204 08 08125XXXXX - Netherlands (Kingdom of the Netherlands) - KPN - KPN Mobile The Netherlands B.V.
228 02 13145XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15024XXXXX - Switzerland - Sunrise - Sunrise Communications AG
208 10 10894XXXXX - France - SFR - Altice
228 02 13025XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 35481XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13025XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 43562XXXXX - Switzerland - Sunrise - Sunrise Communications AG
208 01 15070XXXXX - France - Orange - Orange S.A.
228 02 13148XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15026XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 43562XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15026XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 43562XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13025XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13147XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 35466XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13329XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 16020XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13151XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15031XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13151XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 15032XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13123XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13037XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13151XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13037XXXXX - Switzerland - Sunrise - Sunrise Communications AG
228 02 13151XXXXX - Switzerland - Sunrise - Sunrise Communications AG



6
Recherche par le design II : Vers des objets de contestation

Comme je l'ai déjà évoqué, de nombreux journaux ont au cours des années 2010 relaté la survenance d'interactions étranges avec des téléphones mobiles dans les manifestations ainsi que l'apparition d'appareillages inhabituels montés sur des véhicules d'intervention. Ces occurrences sont symptomatiques de l'utilisation d'IMSI catchers. L'utilisation de tels dispositifs à des fins de surveillance de manifestations a été rapportée depuis quelques années (Parks, 2016). Après avoir achevé l'étape de reconstitution, plusieurs questions sont apparues : comment peut-on concevoir un objet de contestation et de contre-offensive pour questionner un objet si controversé ? Comment un objet pourrait-il fonctionner de manière collective afin de manifester son opposition ? Quel est le potentiel politique d'un tel objet de design critique ? Ce chapitre présente (1) des objets de contestation et des stratégies possibles pour résister face à la surveillance ; (2) les résultats du workshop *900 MHz: Protest*, donné auprès des étudiants du master Media Design de la HEAD — Genève en octobre 2019 ; et (3) expose la conception d'un objet désobéissant — le *BlocBalloon*, la façon dont cet objet pourrait fonctionner et quels types d'interaction il amène ainsi que son potentiel politique[51].

6.1 Des objets de contestation

Comme nous avons pu le voir dans l'introduction, les IMSI catchers sont souvent utilisés dans les manifestations, comme lors des manifestations anti-gouvernement en Ukraine (2013) ou Black Lives Matter (2020). En outre, dans un court reportage de Vice News (2016)[52], Richard Tynan de Privacy International montre à l'aide de matériel et de logiciel dédiés la présence d'antennes relais illégitimes émettant à proximité des manifestations anti-austérité à Londres, ainsi que l'émission d'un signal inhabituellement élevé venant des Chambres du Parlement. Plus récemment, pendant les manifestations de Hong Kong, il était conseillé aux participants d'acheter des cartes SIM prépayées[53,54] puisqu'ils pouvaient potentiellement être suivis à travers leur téléphone. Tous ces exemples constituent une preuve de l'utilisation des IMSI catchers par les forces de l'ordre. Bien que le contexte de la manifestation ne soit pas le seul dans lequel les IMSI catchers sont utilisés, nous nous concentrerons principalement sur celui-ci pour le reste du chapitre.

51 Ces objets couvrent les attaques à l'encontre des réseaux 2G (qui relève majoritairement du protocole GSM) et ne couvre pas les attaques 3G et 4G. Néanmoins, il est possible de forcer les téléphones mobiles à "tomber" sur le réseau 2G (par exemple avec des brouilleurs) et ainsi viser les téléphones 3G/4G.

52 <https://www.youtube.com/watch?v=rzBWoVh4qhk> consulté le 15.02.2022

53 <https://twitter. com/MashaBorak/status/1138781859939176448> consulté le 15.02.2022

54 <https://chicago.cbslocal.com/2014/12/06/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/> consulté le 15.02.2022

Après avoir reconstitué un IMSI catcher, la question que je voulais aborder était comment les perturber afin de questionner leur légitimité ; en tant que chercheur dans les champs de l'art et du design, je voulais le faire à travers la conception et la production d'un objet. En 2014, l'exposition *Disobedient Objects* au Victoria & Albert Museum commissionnée par Catherine Flood et Gavin Grindon (Flood, Grindon, 2014) montrait une collection d'objets qui explorait « la culture matérielle du changement radical et de l'opposition ». Ces objets étaient principalement conçus par des manifestants pour des manifestants, ils comprenaient des masques anti-lacrymogènes, des dispositifs de verrouillage, des boucliers-livres, des *sound systems* et des gonflables (sur lesquels je reviendrai plus en détail par la suite), impliqués avec succès dans des actions tactiques et stratégiques. Pour Flood et Grindon, ceux-ci « peuvent être simples par les moyens, mais ils sont riches dans leurs fins ». En effet, la plupart d'entre-eux utilisaient des objets du quotidien modifiés afin d'accomplir un nouvel objectif ; certains d'entre-eux étaient décrits dans des « How-To Guides » afin de réaliser sa propre version. En 2016, le chercheur Garnet Hertz reprend le terme « disobedient » et l'applique à l'électronique. Ainsi dans *Disobedient Electronics : Protest* (Hertz, 2016), Hertz compile une collection d'objets électroniques afin de protester contre, perturber, défaire et combattre des sujets divers comme la surveillance, le non-respect du droit à la vie privée, les lois anti-avortement ou encore la l'inégalité salariale homme-femme. Il souligne que « concevoir des objets électroniques peut être une forme efficace de débat social ou d'opposition politique ». À l'opposé des objets présentés au V&A, les *disobedient electronics* endossent une dimension plus technologique, impliquant des bouts de code et des éléments électroniques. Est-il possible d'utiliser l'électronique pour s'opposer la surveillance téléphonique mobile, éventuellement en retournant la technologie de l'IMSI catcher contre lui-même (par exemple en utilisant les mêmes failles du protocole GSM sur lequel il repose) ?

Le chercheur en *surveillance studies* Gary T. Marx détaille « *eleven easy moves* » (Marx, 2003) pour neutraliser la surveillance : *discovery moves, avoidance moves, piggy-backing moves, switching moves, distorting moves, blocking moves, masking (identification) moves, breaking moves, refusal moves, cooperative moves, et counter-surveillance moves*. Il est possible de reprendre certains d'entre eux pour penser des objets désobéissants contre la surveillance du réseau GSM. Dans le cas de l'IMSI catcher, quelques options afin d'éviter d'être individuellement ciblé par une fausse antenne relais apparaissent comme évidentes. La première, la plus triviale, serait de ne pas avoir de téléphone (ce qui ne semble pas raisonnable dans un contexte de manifestation) ou de l'éteindre — c'est un « *avoidance move* ». Utiliser une barrière de blindage électromagnétique pour le ranger peut aussi être considéré comme une alternative analogique. Une option plus radicale serait d'utiliser un brouilleur pour rendre les fréquences inutilisables pour les

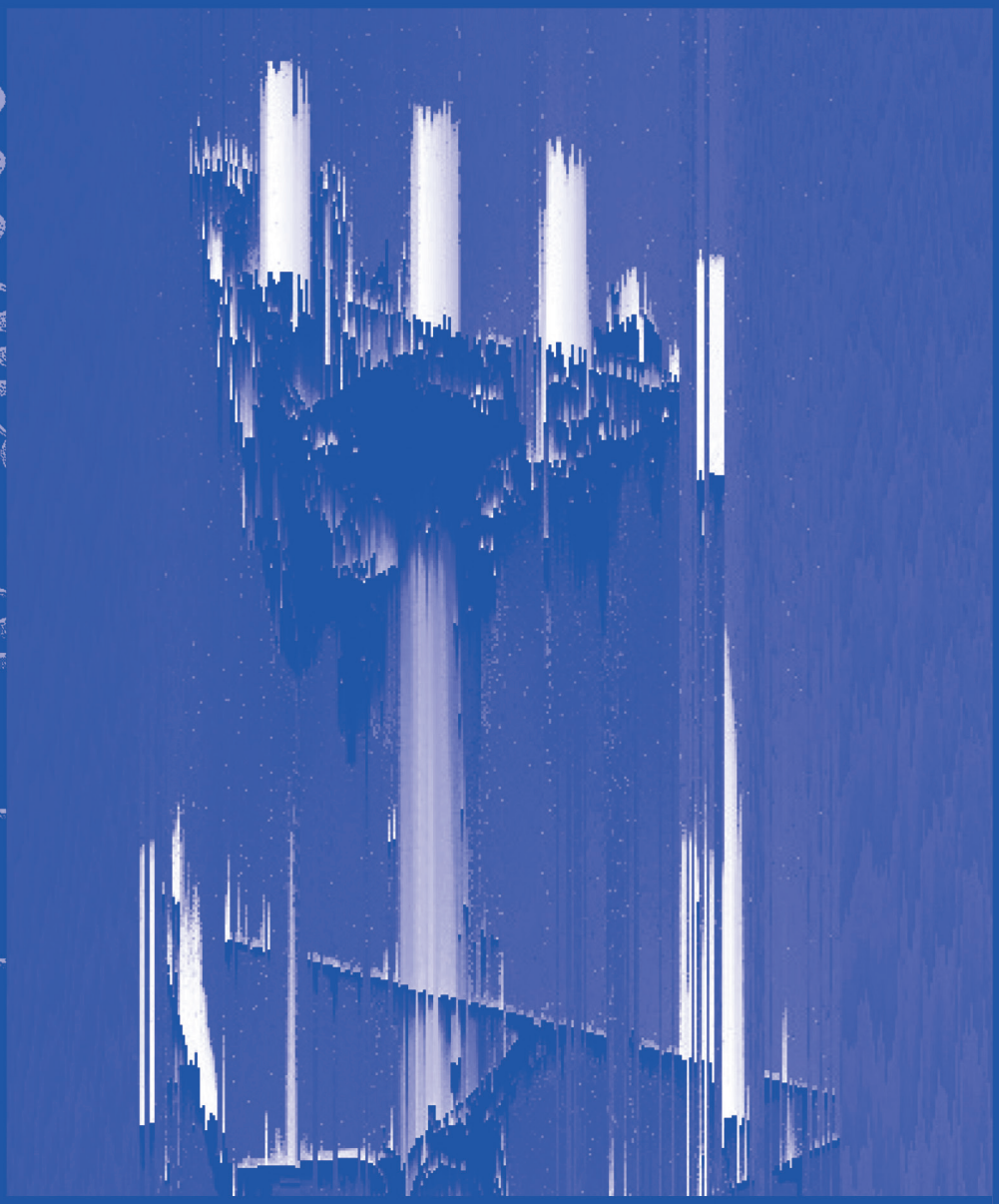
communications GSM, un « *blocking move* » hautement illégal dans la plupart des cas. En outre, le conseil aux manifestants hongkongais d'utiliser un téléphone jetable et une carte SIM prépayée afin que leur identité ne soit pas associée à leur IMSI se révèle souvent impossible dans certains pays sans devoir présenter une carte d'identité (comme c'est le cas en France et en Suisse par exemple). Une autre option est d'utiliser la 4G — comme noté précédemment, l'attaque exécutée par les IMSI catchers est efficace sur les réseaux 2G — uniquement avec des applications dédiées et chiffrées de bout en bout, malheureusement seulement quelques téléphones ont actuellement une option qui permet de forcer les communications 4G ; ceci serait associé à un « *blocking move* ». Voyons maintenant comment certains de ces *moves* peuvent entrer dans la conception d'objets de protestation.

6.2 Workshop 900 MHz: Protest

Le workshop *900 MHz: Protest* a été donné du 28 octobre au 1er novembre 2019 auprès de 7 étudiant.e.x.s de deuxième année du Master Media Design. Je présente dans cette partie la méthodologie employée ainsi que les résultats obtenus.

Méthodologie

Le workshop a débuté sur un exposé de l'utilisation de l'IMSI catcher en manifestation, puis sur la présentation de différentes tactiques de détection, de contre-attaque et de contre-surveillance comme celles présentées plus haut, ainsi que des exemples issus du domaine militaire, de la finance ou encore du monde animal. S'en est suivi une partie plus technique dédiée à la présentation du protocole de communication GSM, d'outils pour explorer le réseau téléphonique mobile (*Software Defined Radio*, outils analogiques) et à une série de petites expérimentations sur le réseau : écoute passive de l'activité sur la bande de fréquence 900 MHz, déploiement d'un *cell-site simulator* qui a permis l'envoi de messages et d'appels téléphoniques sur un réseau GSM local. Les IMSI catchers reconstitués dans la partie précédente ont aussi été présentés aux étudiants. Les questions posées aux étudiants étaient les suivantes : quels enjeux soulève l'utilisation de l'IMSI catcher en manifestation ? Comment sont exploitées les données collectées par de tels systèmes ? Quels objets pouvons-nous concevoir pour questionner leur légitimité ? Le résultat de ce workshop est une série de projets qui abordent la prévention, la détection, la protection et la perturbation de la surveillance du réseau téléphonique mobile, dont la plupart prennent place dans un contexte de manifestation dans l'espace public urbain. Ceux-ci ont été présentés sous la forme d'un fanzine (pp.141-156).



006 Hacktivist

– cupidon –

– the surveillance tagger ki

– data war –

– mega-blast –

– the ghost cell catcher –

900 MHz: protest

900 MHz is the frequency band used for GSM communications.

This publication shows the results of a one-week workshop conducted with MA Media Design students at HEAD – Genève.

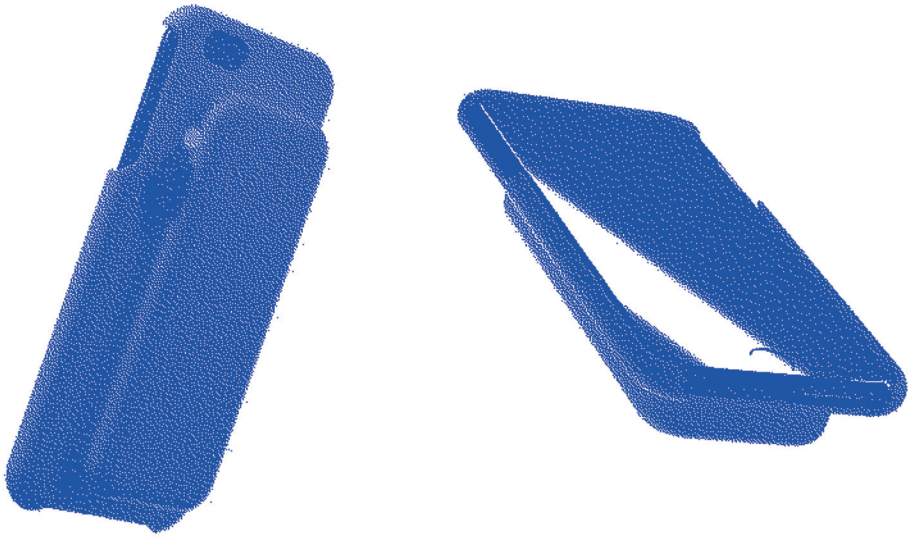
Taking digital and electromagnetic surveillance as a starting point, we focused on the case of the IMSI catcher: a device mimicking the activity of a cell tower to intercept data and communications of cellphones connecting to it. What issues raises the use of such a device ? How are used data collected by such systems ? What objects can we design to question their legitimacy ?

The workshop introduced a case study of digital surveillance, by exploring not only cellular networks with open-source tools, but also means of protestation and counter-surveillance in front of such devices through cryptography, camouflage, obfuscation and the use of decoys. Students then conceived prototypes that question the use of IMSI catchers, while imagining scenarios that explore the potential future of these objects. The result is a series of projects that tackle prevention, detection, protection and disruption of the mobile network surveillance, most of them taking place in an urban protest context.

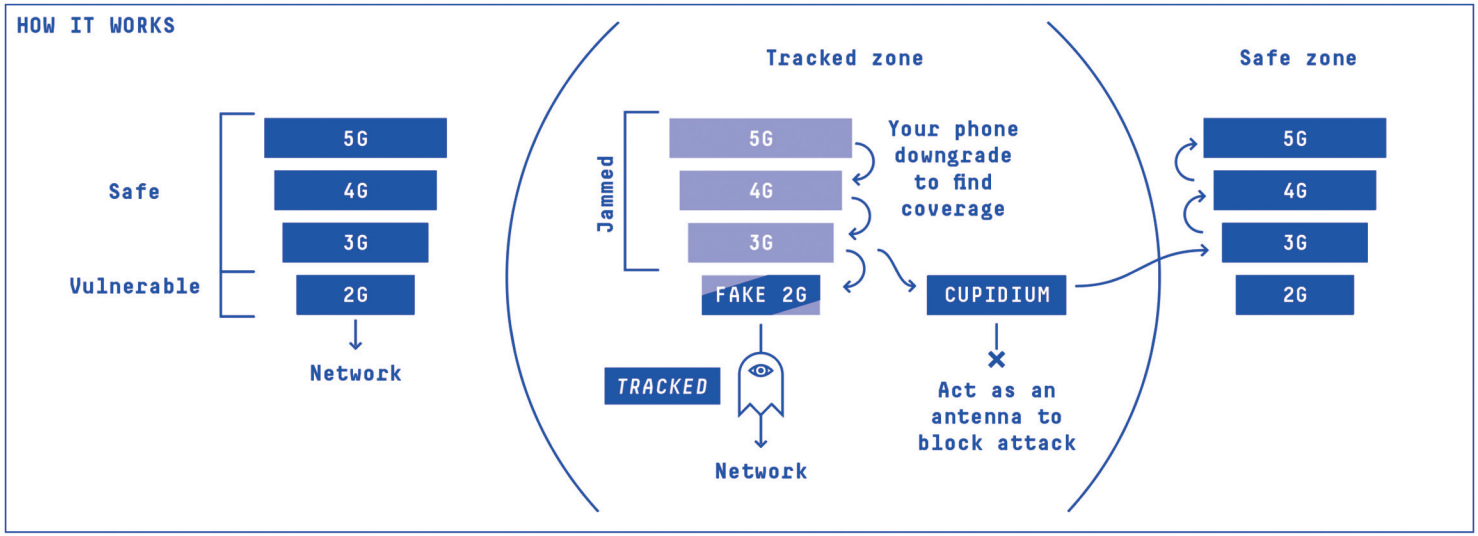
November 2019

— cupidium, a self imsi cacther safe zone —

An open project that aim to make you invisible
to third party eyes.
It is a phone case, prenventing Man in the Middle
attack on your phone, keeping your connection safe
and thus making you untrackable.
This project rely on small electronics and
3D printing. It is build upon CalypsoBTS,
an open-source code turning cheap phones into
GSM network front-ends.



Théo Francart and Vincent Belet



INSTRUCTIONS

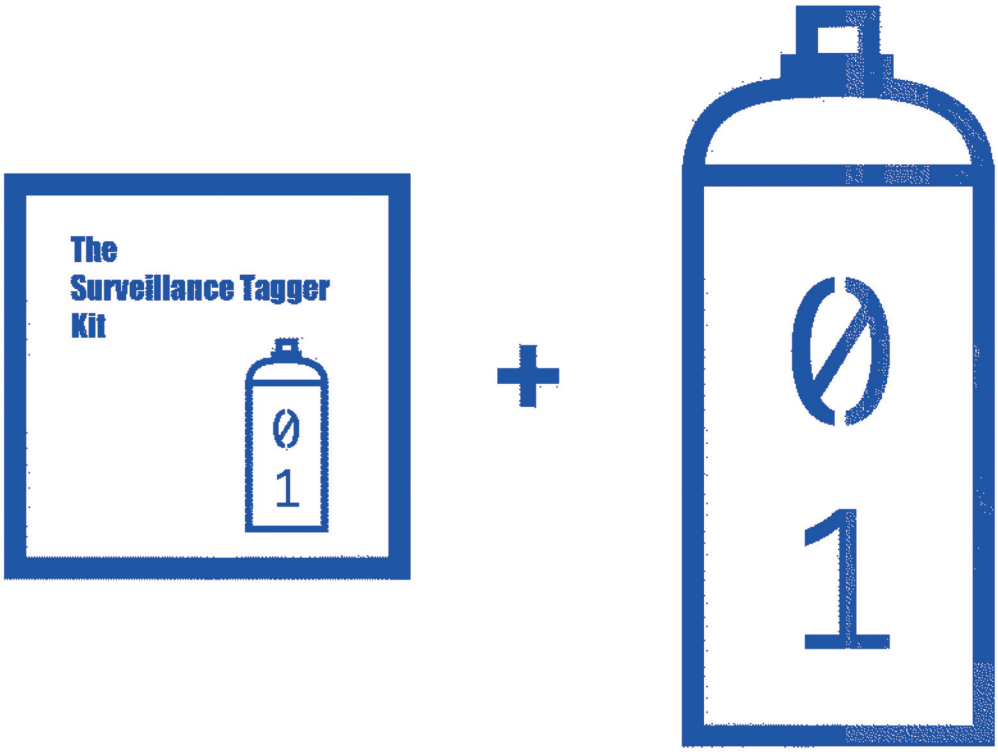
1. To build your own CUPIDIUM,connect to github.com/cupidium and follow instructions. You will need an old phone (like Nokia 3310) and a 3D printer.
2. Turn it on when you do not want to be tracked.
3. You're good to go.

– the surveillance tagger kit –

02

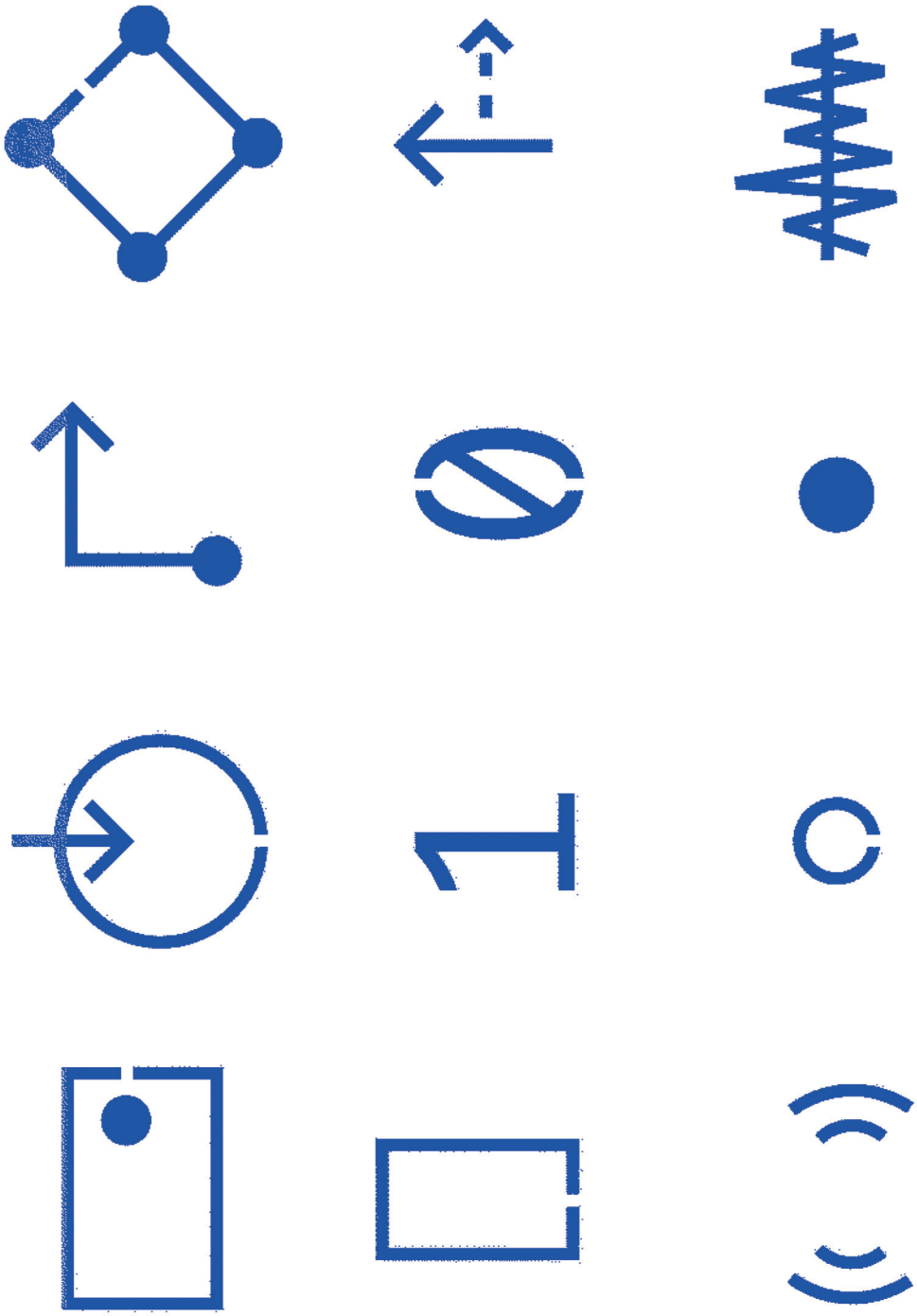
The kit is aimed to turn visible the imperceptible surveillance devices used against citizens.
It focuses on the threat comming from telephonic communication, gps, wi-fi and camera.
It uses a graphic code to help understand precisely what kind of surveillance device is used to steal the data.

Users are invited to tag the places that might be monitered by using stencil and spray paint.
Those places are then considered unsafe and users are invited to avoid using their device to protect their personnal data.



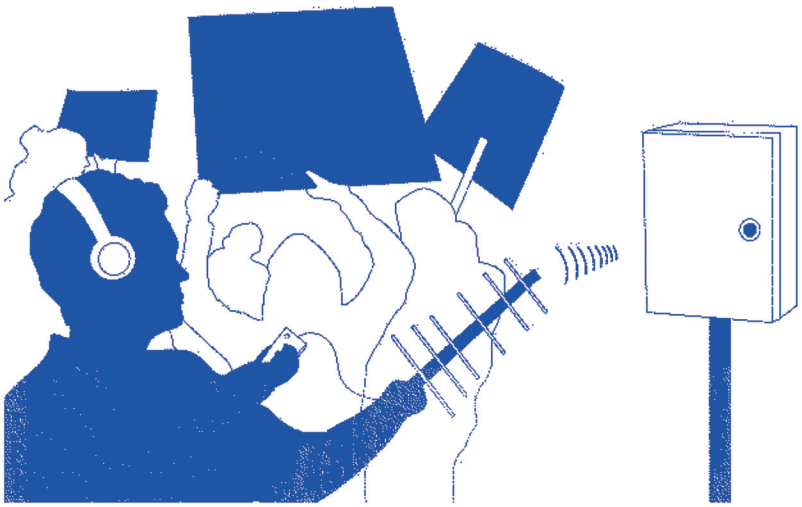
Léa Lansiaux

The kit is available online and reproducible using cardboard or paper.

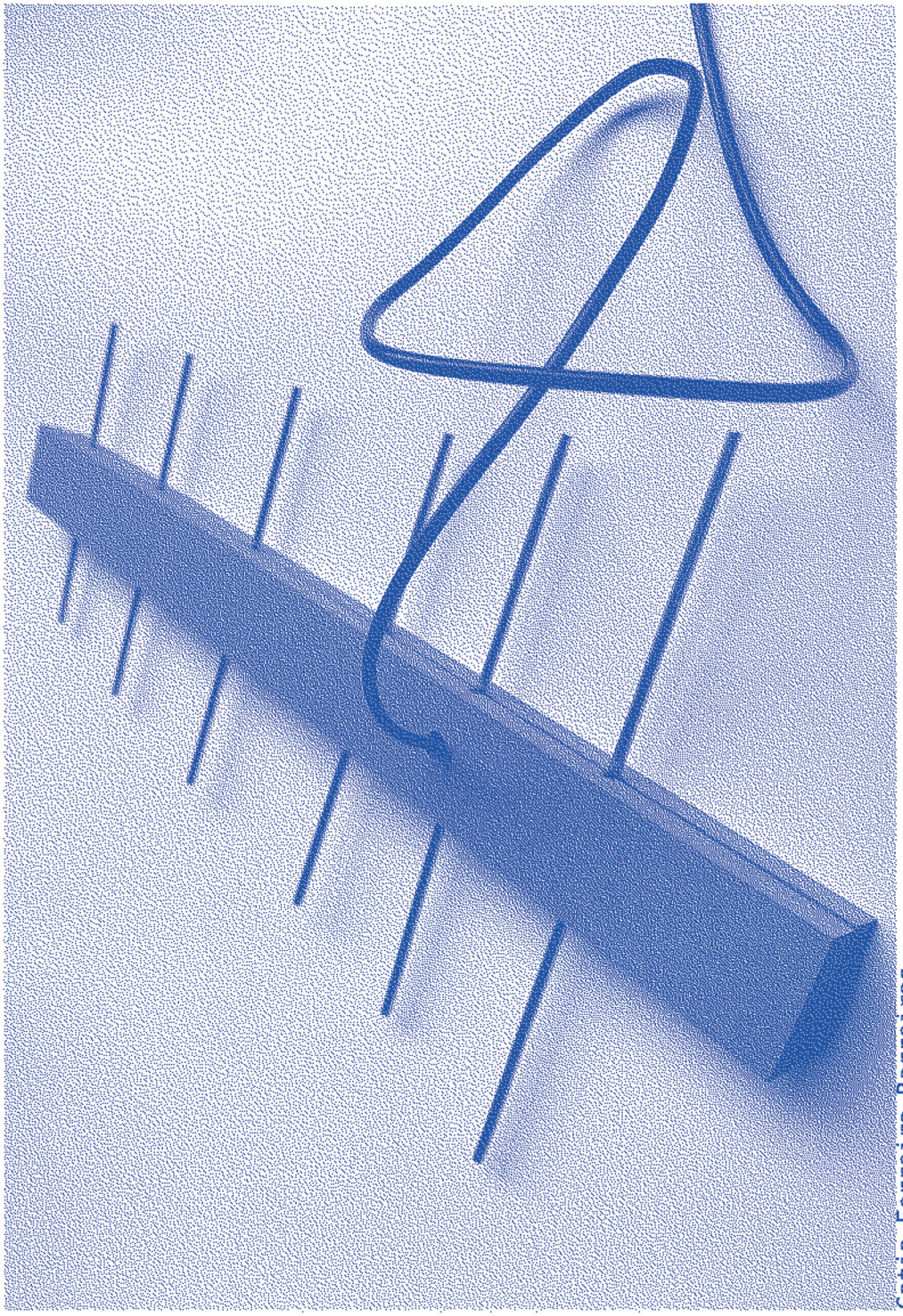


– the ghost cell catcher –

The Ghost Cell Catcher is a device you can build yourself from scratch and take with you during protests to detect the presence of IMSI Catchers. The tool is a combination of a Yagi antenna that captures 900 MHz frequency and a sound amplification system that allows you to hear it. Pointing the antenna towards street furniture like electrical boxes, trash cans or anything that appears suspicious is a way to verify there’s not hidden ghost cells in there, that way you can continue to protest peacefully with the awareness that you’re not being monitored by anyone.



03



Catia Ferreira Barreiras

— data war —
///

If the 2016 Olympic games in Brazil are viewed as a “success,” it may hide an even greater success for the international surveillance industry. As part of its already dubious legacy, marred by police brutality in poor neighborhoods and the eviction of thousands of families, the Rio Olympics will leave in its wake a more-equipped police and Armed Forces and a completely monitored city, which may become a national standard. The lack of transparency and proper regulation for limiting the use of the newly acquired technology is a perfect recipe for more human rights abuses. Unfortunately, surveillance technology for the Olympics doesn’t often just go away. Instead, it’s re-purposed for law enforcement” or other domestic uses.

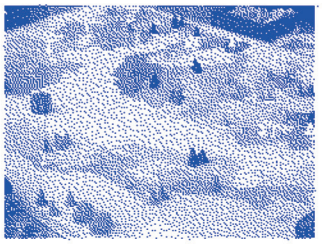
// Project Proposal

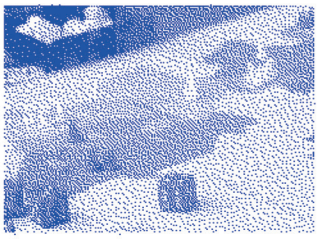
The proposal is a board game based on the game “La Conquete du monde” (AKA Risk or WAR). The game has the same rules as the original game but with different missions: instead of armies to conquer territories, there will be surveillance devices such as IMSI Catcher, Cameras, vigilant balloons, drones, jammers, etc. The missions will be made on the map of Rio de Janeiro, Brazil, a city that since the advent of the Olympics has been using a wide surveillance apparatus arbitrarily.

Some critical points of the city were chosen to be conquered: The huge IBM’s information center located in the center of the city, the ‘militias’ that settle in the Favelas and intercept ordinary citizens houses, and some public spaces that are stages of great manifestations and are recurrently under monitoring.

Players must then reclaim these spaces by using new technological devices against the arbitrary performance of the city or by destroying them.

In addition, the game has information cards about certain surveillance devices in the city.As in the original game, the first to conquer the territories mentioned in the mission card wins. Also, armies were replaced by IMSI Catchers Vans.



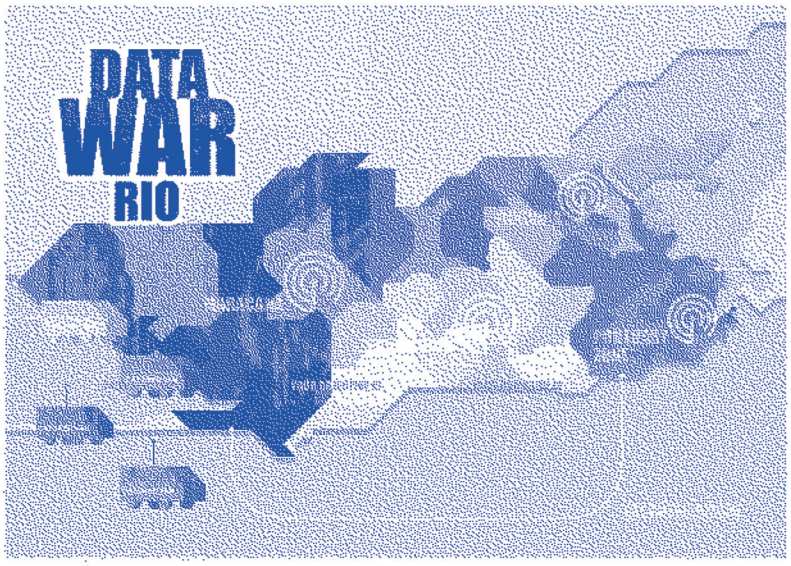


04

// Who: Children / Teenagers

// Why: The goal of the game is to spark debate about how governments have been watching people in invisible ways, with arbitrary laws and no democratic decisions. It's a way to prevent and educate about new technological gadgets that are mostly unknown to the general population.

// Where: The application of the game is free and can also be used by teachers in schools. Just print the board size in A2, the cards are available in A4 size and the attack/defense pieces and dices can be made using the templates available on the site.



make your own game. it's free!
print at: laiskunzendorff.com/900mhz

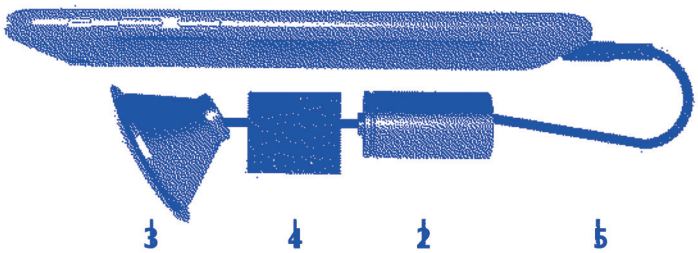
Laïs Kunzendorff

— mega-blast —
///
IMSI destruction tool for protesters.This device turns your phone into massive emitters of GSM signals that spread your messages and saturate surveillance tools.

Getting Started

What do you need :

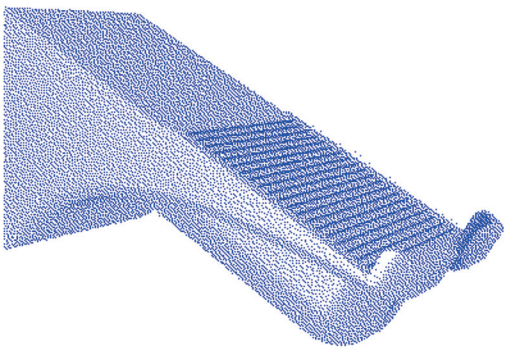
—lithium Batterie 2
—speaker 3
- amplifier 4
—smartphone connecter 5

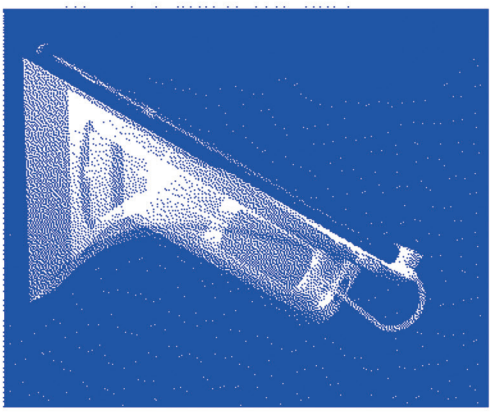


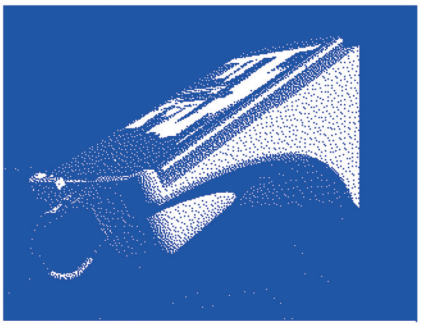
Download:

You can download the files on the following URL:
https://github.com/megablast/megablast

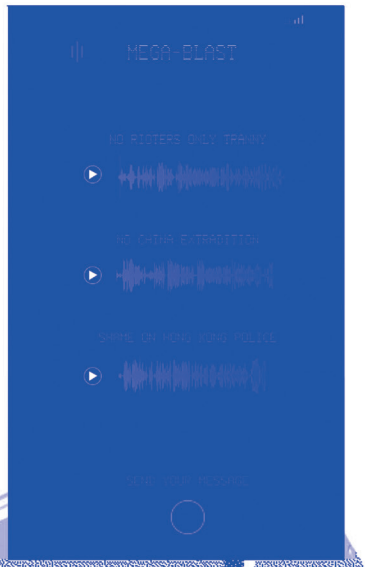
Print the 3D model MBstruc.stl on the megablast folder, then put inside all the electronics components



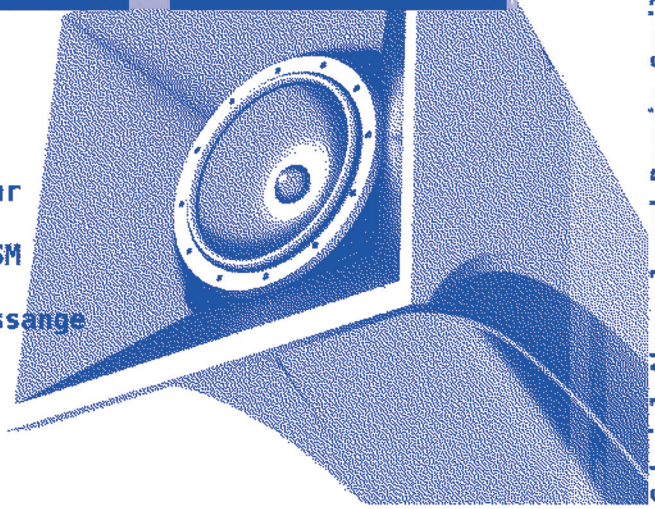




link it with your phone, then instal megablast.apk from the megablast-api folder.



now you can use the mega-blast, record your message and send him by thousands to the GSM network. you can also send a pre written messange from your community.



Gabriel Abergel and Romain Graille

900 Mhz Protest
directed by Félicien Goguey

Gabriel Abergel
Vincent Belet
Théo Francart
Catia Ferreira Barreiras
Romain Graille
Laïs Kunzendorff
Léa Lansiaux

28.10.2019 – 01.11.2019

Cupidium : A Self IMSI Catcher Safe Zone (Vincent Belet, Théo Francart, pp.144-145) est un objet pertinent puisqu'il incarne physiquement un moyen de protection individuelle contre la surveillance qui trouve sa place dans les *blocking moves* de Gary T. Marx. Ainsi, il pose une bonne base pour explorer sa fonction et la potentielle communication autour de celui-ci. Toutefois, il se limite à un artefact imprimé en 3D qui n'explore pas pleinement le potentiel narratif de l'objet ainsi que le contexte dans lequel il est utilisé. Enfin, la description technique superficielle est assez peu vraisemblable et ne donne pas assez de crédit au dispositif.

The Surveillance Tagger Kit (Léa Lansiaux, pp.146-147) présente une design fiction qui donne à voir par un langage codifié. L'objet produit permet de formaliser cette fiction et d'imaginer ses usages ; ainsi, le kit est constitué de pochoirs et d'une bombe de peinture permettant de signaliser une potentielle surveillance et en ce sens permet la réalisation de *avoidance moves*. Néanmoins le caractère éphémère et temporel du médium utilisé n'est pas abordé et laisse perplexe face à une surveillance « liquide » (qui est mobile et flexible).

The Ghost Cell Catcher (Catia Ferreira Barreiras, pp.148-149) est un objet DIY singulier qui permet la détection de dispositifs de surveillance GSM dissimulés dans le mobilier urbain de manière tout à fait analogique. Le processus de recherche par la pratique est basé sur une démarche pertinente : refaire pour comprendre, qui permet de saisir certains enjeux liés à la surveillance et aux modes de fonctionnement de l'IMSI catcher (émission, camouflage, etc). Il s'apparente au *Discovery Moves* de Gary T. Marx et prend tout son sens dès lors qu'on le positionne dans un contexte plus large, en conjonction avec d'autres moyens de détection (logiciels par exemple) et de prévention (cartographie ou marquage, comme dans le projet précédent).

Data War (Laìs Kuzendorff, pp.150-151) adopte une approche singulière vis-à-vis d'un sujet difficile à aborder, il reprend la forme d'un jeu de plateau relativement connu (Risk), pour l'appliquer à des enjeux dont on parle peu dans une perspective pédagogique et ludique. Les mécaniques du jeu et les interactions entre les joueur permettent d'apprendre sur la surveillance. En ce sens, ce n'est pas directement un objet de contre-surveillance et ne trouve pas sa place dans les *moves* de Marx ; toutefois, il permet d'amener une forme de prévention autour des différents enjeux de la surveillance.

Mega-Blast (Gabriel Abergel, Romain Graille, pp.152-153) est un projet pensé dans un contexte clairement défini (manifestations de Hong-Kong), le prototype réalisé permet d'exposer son principe d'interaction. Celui-ci, techniquement vraisemblable pose des questions pertinentes vis-à-vis de l'objet IMSI catcher

avec l'utilisation d'une stratégie singulière dans ce cas (DDoS). L'intégration du dispositif dans un mégaphone, objet que l'on retrouve communément dans les manifestations, en fait un objet plausible qui se concrétise à travers deux principes d'interaction complémentaires. Pour aller plus loin, il aurait été pertinent d'explorer les dynamiques de fonctionnement en réseau (à qui envoie-t-on les messages ? comment synchronise-t-on le service ? combien d'utilisateurs y a-t-il au moment donné ?). Il fait appel aux *distortion moves* d'une part, il ne fonctionne que comme un *cooperative move* et il est nécessaire qu'il soit adopté par un grand nombre de manifestants d'autre part.

Ainsi, ce workshop a permis de concevoir cinq objets de contestation et d'explorer un ensemble d'hypothèses assez large dans des formes singulières et diverses, mettant en œuvre différentes stratégies de résistance. Toutefois, ils sont pour la plupart à l'état de concept ou d'artefact non fonctionnel et à l'exception de *Mega-Blast* ils sont souvent destinés à être utilisés de manière individuelle. Qu'en est-il si l'on commence à penser à une option plus collective — dans les mots de Marx un « *cooperative move* » — qui pourrait être appliquée dans le cas spécifique de la manifestation et concernerait tous les manifestants à portée ? Quel serait un tel objet désobéissant qui perturberait collectivement la surveillance GSM ? J'essaierai de répondre à ces questions dans la suite de ce chapitre en prenant des exemples de stratégies tactiques pour s'opposer à la surveillance basés sur l'obfuscation et en présentant un objet désobéissant que j'ai conçu à l'échelle 1:1 : le *BlocBalloon*.

6.3 BlocBalloon : concevoir un objet de contestation contre la surveillance du réseau GSM

Obfuscation et gonflables

Obfuscation

Une approche stratégique pour cacher quelque chose aux yeux d'un système de surveillance — ou pour le perturber — est l'obfuscation. À son niveau le plus basique, l'obfuscation consiste à cacher une véritable information (ou un véritable signal) dans un ensemble d'informations fausses ou erronées ; ceci peut être atteint de différentes manières. Prenons quelques exemples qui illustrent ce principe et qui présentent différentes approches de l'obfuscation.

Depuis la Seconde Guerre mondiale, une technique appelée « *chaff* » a été utilisée comme contre-mesure à l'encontre des radars pour dissimuler des aéronefs. L'avion relâche à un moment donné de fines pièces d'un matériau réfléchissant comme de l'aluminium et de la taille de la moitié de la longueur d'onde du radar, ainsi le signal

du radar est réfléchi dans une multitude de points. Au lieu de cacher l'avion, cette technique donne à l'opérateur du radar une myriade de cibles potentielles autour de l'aéronef toujours présent, faisant ainsi échouer la surveillance de l'espace aérien. Cette technique « exploite le champ limité de l'observateur » en se basant sur ses limitations techniques (Brunton, Nissenbaum, 2015). Une telle approche est seulement efficace si l'« obfuscateur » connait extrêmement bien les outils utilisés par l'observateur ; par conséquent, l'« obfuscateur » n'a nul besoin d'envoyer une flotte entière d'aéronefs pour faire diversion, mais peu simplement utiliser sa connaissance du système de surveillance pour lancer des leurres adaptés.

Un exemple plus récent (et plus proche de notre objet d'étude) est la technique de « battage des cartes SIM » afin de rendre le ciblage mobile incertain (Brunton, Nissenbaum, 2015, p. 18). Comme Brunton — professeur de médias, culture et communication — et Nissenbaum — professeur des sciences de l'information — l'énoncent dans leur livre, les drones utilisent les métadonnées des téléphones mobiles (en l'occurrence l'IMSI) et leur propriété géolocatives pour cibler leurs victimes : cela « repose finalement sur les cartes SIM et la possession physique de téléphone mobile — une sorte d'étroite bande passante qui peut être exploitée ». Dès lors, une contre-offensive ou contremesure possible et simple consiste à redistribuer au hasard les cartes SIM entre les individus. En ce sens, « utiliser l'obfuscation pour mélanger et mixer les signaux, plutôt que de générer des faux, peut offrir une mesure de défense et de contrôle » (Brunton, Nissenbaum, 2015, p. 19). Cette technique, qui s'apparente aux « Switching Moves » de Marx, pourrait aussi être utilisée par des activistes et leurs pairs avant une manifestation, nous verrons juste après comment elle pourrait être améliorée dans le cadre d'une surveillance conduite à l'aide d'un IMSI catcher.

En plus des IMSI catchers, la Loi sur le renseignement de 2015 en France légalise l'utilisation de « boîtes noires » sur le réseau Internet pour traquer des « comportements suspicieux ». À la suite du vote de cette loi (et du manque de débat public), j'avais conçu dans un projet antérieur à cette thèse *Masquerade*[55], une pièce de design critique qui repose elle aussi sur l'obfuscation. Elle est composée d'un réseau de petits ordinateurs qui s'envoient constamment des messages suspicieux basés sur des dictionnaires de mots-clés prétendument déclencheurs et qui sont supposés perturber la surveillance conduite sur Internet. Bien qu'il n'existe aucune manière d'évaluer son efficacité tout en étant hautement spéculative — puisque nous ne savons pas exactement comment ces boîtes noires fonctionnent — cette pièce repose aussi sur un principe d'obfuscation. Si le moyen d'action est similaire aux exemples précédents, la finalité ici n'est pas de noyer des messages suspicieux ou criminels dans un volume de faux positifs, mais plutôt d'utiliser l'obfuscation comme une manière de protester et de défendre son droit au respect de la vie privée.

55 <https://felicien.io/masq/> consulté le 15.02.2022

Chaque citoyen qui installe le système à domicile déclare haut et fort sur le réseau : « je ne suis pas d'accord ». C'est une manifestation constante sur le réseau pour signifier son désaccord et réclamer son droit à la vie privée. Tout d'abord conçu pour être distribué sous une licence libre et open source, *Masquerade* a seulement été présenté dans des expositions comme une pièce de design critique dans le but de susciter le débat (non-existant au moment de sa création), tout en créant une fiction dans un espace de design spécifique.

Gonflables : de la Seconde Guerre mondiale aux manifestations

Tout comme l'utilisation des « *chaffs* », un autre exemple d'obfuscation pendant la Seconde Guerre mondiale était le recours à des objets gonflables. Ces gonflables étaient stratégiquement placés — respectivement par les camps Alliés et de l'Axe — comme des leurres pour tromper l'ennemi sur les ressources militaires à leur disposition. La *Ghost Army*, un corps spécial de l'armée américaine composé d'artistes et d'illustrateurs[56], avait recours à la duperie visuelle en transformant des objets gonflables en chars et avions factices, mais aussi à d'autres techniques comme la duperie sonore ou la duperie radio eux-mêmes utilisés dans les champs plus larges de la tromperie militaire et la guerre de l'information.

L'histoire des gonflables ne s'arrête pas là, puisqu'ils apparaissent aussi dans les années 1930 en Union Soviétique dans un contexte totalement différent : ils étaient notamment utilisés dans des parades à Moscou à l'occasion de célébrations. Artur Van Balen, membre de l'ancien groupe Eclectic Electric Collective et maintenant de Tools for Action, décrit : « la figure du gonflable abordait de nombreux thèmes de la démonstration du progrès technologique avec de nouveaux ballons météorologiques high-tech, à leur utilisation comme symboles de la production réalisée par les ouvriers d'un corps de métier en particulier. Ils créaient aussi des gonflables pour ridiculiser leurs opposants politiques »[57].

Dans son essai *The Inflatable Moment : Pneumatics and Protest in '68*, Marc Dessauce « spécule sur la fonction symbolique des objets gonflables dans des narrations utopiques et durant des moments révolutionnaires » (Dessauce, 1999). Il relate l'utilisation de gonflables dans l'architecture du groupe UTOPIE pour contester les conventions architecturales enseignées à l'École des Beaux-Arts. Au même moment, les gonflables étaient récupérés dans des manifestations, comme lorsque le collectif italien UFO a commencé à utiliser des gonflables pendant les manifestations étudiantes de 1968 à Florence « pour rivaliser avec les monuments et l'architecture historique »[58]. Le collectif UFO occupait la faculté d'architecture

56 <https://www.smithsonianmag.com/history/when-an-army-of-artists-fooled-hitler-71563360/> consulté le 15.02.2022

57 <https://www.vam.ac.uk/blog/disobedient-objects/tools-for-action-interview-with-artur-van-balen> consulté le 15.02.2022

58 <https://floatingutopias.org/stories/lapo-binazzi-artur-van-balen/> consulté le 15.02.2022

et produisait de nombreux *happenings* dans lesquels ils utilisaient des gonflables, l'un d'entre eux représentait un missile-dentifrice avec les mots « Colgate con Vietcong » inscrits pendant une manifestation contre la guerre du Vietnam.

Depuis, les gonflables ont été utilisés dans un nombre considérable d'endroits et dans formes variées. Un des objets désobéissants présentés au V&A était le *Giant Cobblestone* du Eclectic Electric Group. Le collectif utilisait la figure du gonflable afin de perturber le rapport de force habituel entre les manifestants et les forces de l'ordre en utilisant ces pavés géants comme des ballons inoffensifs. Van Balen rapporte, « les accessoires gonflables, ou gonflables, peuvent transformer une marche de protestation ennuyeuse en un événement ludique, mémorable et interactif »[59]. Ces gonflables n'endossent plus le rôle de leurres, mais portent plutôt le symbole d'une cause à défendre.

59 <https://www.beautifultrouble.org/toolbox/#/tool/inflatables> consulté le 15.02.2022

Fig. 57. Félicien Goguey. *BlocBalloon*. 2020. Vue de l'exposition Ausstellung Schweizer Medienkunst: knowbotiq, Alan Bogana, Félicien Goguey - Pax Art Awards 2019, HeK (Haus der elektronischen Künste Basel). Photo: Gina Folly

BlocBalloon : une antenne relais pirate gonflable

Afin de protester contre le ciblage des téléphones portables pendant les manifestations, j'ai conçu un objet désobéissant qui repose sur l'obfuscation électronique et qui prend la forme d'un gonflable. L'idée derrière *BlocBalloon* est d'avoir un moyen de défense collectif et d'opposition à la surveillance GSM. La pièce a été exposée à la Maison des arts électroniques (HeK) de Bâle à l'occasion de l'exposition Swiss Media Art du 27.05 au 02.08.2020[60]. C'est un objet désobéissant qui perturbe la surveillance opérée par les IMSI catchers en leur montrant de faux IMSIs dans une zone donnée. J'exposerai son fonctionnement dans un premier temps, puis expliquerai sa forme.

Une antenne relais pirate

La partie hardware consiste en :

- un IMSI catcher actif ;
- un dispositif capable de gérer plusieurs cartes SIM (localement ou en utilisant un serveur SIM distant) — de tels dispositifs peuvent être trouvés sous l'appellation de GoIP (pour GSM over IP) et sont le plus souvent utilisés pour des applications commerciales (télémarketing, envoi de SMS en masse) ;
- une alimentation (ou batterie pour la mobilité).

Le processus d'obfuscation suit les étapes suivantes :

- en amont de la manifestation, l'opérateur doit générer des IMSIs et les inscrire sur des cartes SIM, ceci peut être fait avec des cartes SIM programmables (voir par exemple sysmoUSIM-SJS1<http://shop.sysmocom.de/products/sysmousim-sjs1>), habituellement conçues pour être utilisées dans des picocells GSM low cost et non commerciaux ; alternativement, l'opérateur peut utiliser des cartes SIM anonymes (par exemple des cartes SIM prépayées toujours disponibles dans certains pays) ;
- l'IMSI catcher actif intégré au *BlocBalloon* « attrape » les téléphones mobiles des manifestants à sa portée. Ainsi, les téléphones attrapés ne peuvent plus être attrapés par un autre IMSI catcher (par exemple par un des forces de l'ordre) ;
- à chaque fois que l'IMSI d'un manifestant est attrapé, le dispositif qui gère les cartes SIM programmées le substitue avec un faux IMSI ou un IMSI anonyme ; l'IMSI catcher intégré utilise des filtres afin de ne pas

60 Dans le contexte de restrictions sanitaires dû au COVID-19, il est regrettable de ne pas avoir eu la possibilité de recueillir les réactions directes des visiteurs lors du vernissage et lors de l'exposition, à la fois à propos du *BlocBalloon* mais aussi des autres travaux présentés en lien avec le même sujet.

attraper de faux IMSIs émis par le système ;

- une fois qu'ils sont devenus « invisibles » sur le réseau, les manifestants reçoivent un message les informant qu'ils sont sous la protection du *BlocBalloon* ;
- tandis que le *BlocBalloon* accomplit la même chose que d'éteindre son téléphone, il permet toujours d'utiliser d'autres fonctionnalités de celui-ci comme prendre des photos, filmer ou communiquer via WiFi.

Comme je l'ai écrit précédemment, les téléphones GSM se connectent en priorité aux cellules qui ont le signal d'émission le plus fort ; afin de faire disparaître les IMSIs des manifestants, l'IMSI catcher intégré a besoin d'émettre un signal fort et/ou les manifestants doivent se tenir à proximité. Toutefois, grâce au potentiel de perturbation de l'obfuscation, ce n'est pas un problème majeur : même si certains des manifestants ne sont pas connectés au *BlocBalloon*, les surveillants ne peuvent pas savoir quel IMSI est véritable ou non ; les IMSIs des manifestants sont mélangés à de faux IMSIs rendant ainsi non fiable tout renseignement récolté.

Le *BlocBalloon* offre dans une interaction « passive » avec les manifestants une sorte de bulle de protection dans un « tollé silencieux », dans une invisibilité à la manière de la Ghost Army. Cette interaction passive est associée au « *Masking Moves* » de Marx. En effet, « le masquage implique le blocage en ce sens que l'information originale est protégée, mais cela va au-delà puisqu'il implique l'utilisation de la tromperie en respectant l'identité, le statut et/ou la localisation/localisabilité de la personne ou du matériel faisant l'objet de la surveillance » (Marx, 2003). En ce sens, le *BlocBalloon* cache (ou bloque) les véritables IMSIs des manifestants pour ensuite les remplacer (ou les masquer) avec de faux IMSIs, agissant ainsi comme un déguisement. Même si de véritables IMSIs seraient amenés à être interceptés, les forces de l'ordre ne pourraient pas les différencier des faux, en ce sens le *Bloc Balloon* amène aussi un niveau d'obfuscation contre la surveillance. Enfin, ce dispositif anti-surveillance présente un potentiel de désobéissance ; il offre un point de tension fort face aux IMSI catchers « originaux » : les manifestants ne sont pas toujours avertis de leur usage, et il protège aussi les manifestants sans qu'ils aient besoin de le savoir. De plus, sa forme peut apporter un autre type d'interaction.

Fig. 58. Félicien Goguey. *BlocBalloon*. 2020. Vue de l'exposition Ausstellung Schweizer Medienkunst: knowbotiq, Alan Bogana, Félicien Goguey - Pax Art Awards 2019, HeK (Haus der elektronischen Künste Basel). Photo: Gina Folly

BLOC
BALLOON
BLOC
BALLOON
BLOC
BALLOON

Une antenne relais gonflable

Le gonflable prend la forme d'une antenne relais à l'échelle 1:1 de 7 mètres sur 3 (fig. 57 et 58), et ce pour deux raisons principales. D'une part, d'un point de vue tactique, les gonflables sont extrêmement pratiques puisqu'ils peuvent être transportés dans des valises puis être rapidement déployés une fois gonflés à l'air ou à l'hélium. Dans le cas du *BlocBalloon*, la forme gonflable sert aussi de protection à l'électronique embarquée. D'une autre part, d'un point de vue symbolique, la forme gonflable peut devenir et incarner le symbole d'une cause. De plus, lorsqu'ils sont portés par des manifestants, les gonflables génèrent une interaction active. Van Balen prend de l'exemple de « El Martillo » un marteau de 12 mètres, gonflable et argenté assemblé à Berlin puis envoyé à Cancún pour la marche pour le climat durant la Conférence des Nations Unies sur le Climat (2010). La marche était bloquée aux grilles disposées devant le centre de conférence, quand « soudain un groupe de manifestants a couru avec un marteau géant au-dessus de leurs têtes et a frappé celui-ci contre les barrières de police. En pleine vue de la presse, la police mexicaine a déchiré le gonflable en pièces. En quelques heures, les médias internationaux ont déclaré le marteau gonflable le symbole de la manifestation pour ce jour »[61]. Comme le souligne Konstanze Scheidt, la taille du gonflable force les manifestants à se coordonner dans un mouvement des corps pour le déplacer (Scheidt, 2018) ; c'est aussi dans cette procession que le gonflable possède un potentiel politique élevé, participant ainsi de l'action collective.

Dans le cas du *BlocBalloon*, gonfler l'antenne relais pirate devient un symbole pour retrouver son droit à la vie privée dans l'espace hertzien. Cette vision apporte un second régime de visibilité pour ceux qui savent, la bulle de protection passive figurée par la forme d'une fausse antenne relais devient l'étendard d'une lutte. Sa forme agit à la fois comme un avertissement, qui montre qu'une surveillance téléphonique mobile est potentiellement conduite dans les environs, et indique une contremesure. Cet objet figure la manière dont les IMSI catchers fonctionnent ainsi que la volonté d'opposition à leur utilisation par les forces de l'ordre. Au stade actuel du projet et parce qu'il n'y a aucune manière d'évaluer son efficacité ; plutôt qu'un objet utilisable, le *BlocBalloon* offre un espace fictionnel dans lequel des problématiques liées à un objet spécifique de la surveillance peuvent être discutées.

61 <https://www.beautifultrouble.org/toolbox/#/tool/inflatables> consulté le 15.02.2022

La version hautement symbolique et transparente de l'antenne relais gonflable est dédiée à être montrée dans des expositions ou des espaces muséaux, mais le *BlocBalloon* a d'abord été pensé comme un dispositif anti-surveillance embarqué dans des gonflables « ready-made » — en prenant par exemple des bouées de piscine en forme de flamant rose. Il est ainsi possible d'imaginer que le hardware soit intégré dans des gonflables de formes multiples, symbolisant par conséquent une autre cause mais offrant toujours la même protection. Quelques mois après que le *BlocBalloon* ait été montré à Bâle, des opposants au gouvernement thaïlandais ont utilisé des canards gonflables jaunes devant le parlement à Bangkok[62]. Dans ce cas particulier, les manifestants utilisaient des gonflables de piscine pour se protéger des canons à eau. Si le dispositif *BlocBaloon* y avait été intégré, ces canards auraient aussi pu être efficaces contre les dispositifs de tracking des téléphones mobiles.

Toutefois, le *BlocBalloon* n'a jamais été testé dans des conditions réelles et il n'est pas possible d'évaluer son niveau de protection pour le moment. L'artefact montré dans un contexte muséal a plutôt vocation à ouvrir un espace pour le débat. Le gonflable est présenté accompagné d'une série d'affiches (fig. 59, 60 et 61) qui expliquent sa construction et montre comment il pourrait être reproduit, probablement amélioré et porté dans des manifestations. Ces trois affiches, collées sur le mur comme elles le seraient dans la rue, montre le fonctionnement général du *BlocBallon* et comment il peut-être utilisé en conditions réelles. La première affiche illustre l'effort collectif nécessaire pour porter le ballon, montrant comment il peut être utilisé comme un bouclier contre la répression et la surveillance. La seconde décrit le contexte dans lequel, pourquoi et comment le *BlocBalloon* devrait être utilisé. La dernière explique l'interaction de l'électronique embarquée avec le réseau et les manifestants à l'aide d'un schéma technique.

Le *BlocBalloon* lui-même et les affiches qui l'accompagnent incarnent un scénario potentiel contre la surveillance et déploient un espace discursif dans lequel la nature contestataire de l'objet donne aux manifestants l'opportunité de montrer leur opposition contre la surveillance. Le *BlocBallon* propose des moyens d'action contre la surveillance téléphonique mobile et des moyens d'interaction et/ou de protection face aux forces de l'ordre dans une manifestation en symbolisant cette lutte. Le but ici, plutôt que de contrecarrer effectivement la surveillance, est de susciter une prise de conscience à propos de l'utilisation des IMSI catchers, de susciter un débat à propos de ses dérives potentielles et futurs possibles, et d'apporter une réflexion sur l'usage actuel des IMSI catchers dans la surveillance des manifestations. Enfin, si le *BlocBalloon* était développé un stade plus avancé

62 <https://twitter.com/jcalpickard/status/1329142075288379393> consulté le 15.02.2022

en un dispositif fonctionnel et testé sur le terrain, il pourrait être rapproché de la définition du *adversarial* design de Carl DiSalvo (2012). En effet, dans ce cas, le *BlocBallon* susciterait non seulement une prise de conscience à propos de l'utilisation de la surveillance mais offrirait aussi un moyen efficace de la contourner, devenant ainsi un objet qui questionne les relations entre théorie politique, design et technique et qui offre une nouvelle forme d'expression et d'action politique.

6.4 Du rôle des objets désobéissants

Nous avons pu voir dans ce chapitre que la conception et la production d'objets de contestation permettent de dessiner des trajectoires de sortie et de protestation face à la surveillance du réseau téléphonique mobile et de l'emploi de l'IMSI catcher. En effet, là où les *surveillance studies* dressent le plus souvent un tableau assez sombre et inquiétant de la surveillance, les designers peuvent tester des hypothèses sur de potentielles portes de sortie comme des moyens de prévenir, déjouer, contrer, détourner ou contourner la surveillance. C'est ce que montre la diversité des tactiques utilisées par les étudiant.e.x.s du Master Media Design, qui ont chacun.e.x pu s'approprier le phénomène avec des approches en lien avec leur pratique respective : didactique, pédagogique, individuelle, collective ; cette diversité des productions est soulignée lorsqu'on les confronte au modèle de Gary T. Marx et ses différentes tactiques. Ces objets ont été conçus dans le contexte d'une école d'art et de design, lors d'un atelier, et donc dans un contexte qui spécule sur les possibles, certes plausibles, mais sans lien avec des actions de protestation ou de luttes spécifiques et il serait pertinent de savoir ce qu'ils deviendraient entre les mains d'activistes, de techno-critiques ou de hackers. Toutefois, sans aller dans une réalisation fonctionnelle et sans que les étudiant.e.x.s n'aient de compétences techniques avancées, la simple production de prototypes spéculatifs et leur publication sous forme de fanzine permet de figurer le problème et les enjeux de l'utilisation de l'IMSI catcher dans le contexte de la manifestation. La matière produite dans ce contexte permet aussi d'illustrer la diversité des usages possibles, en rendant tangible des aspects tels que la détection et le brouillage de signaux, la signalisation de la surveillance ou encore l'obfuscation collective.

De la même façon, nous avons vu que prendre la reconstitution d'un objet de surveillance confidentiel comme un point de départ peut permettre d'ouvrir un espace complet pour le design, dans lequel il est possible de développer un objet spéculatif qui questionne la légitimité d'un objet aussi controversé. En se basant sur la reconstitution d'un objet technique, il est ainsi envisageable de créer des outils pour retourner son fonctionnement contre lui-même et de concevoir un objet de contestation afin de contrecarrer et protester contre la surveillance du

réseau. En assemblant des objets désobéissants habituellement rencontrés en manifestations (comme des gonflables) et des tactiques inspirées de l'armée (comme l'obfuscation), il est possible de conceptualiser et produire un objet qui défie la surveillance opérée sans l'espace hertzien qui en retour nous informe sur les IMSI catchers; dans le sens où son mode de fonctionnement « coup de filet » et sans filtre devient ici tangible et où l'on peut se rendre compte de son aspect de surveillance de proximité (directement lié à sa puissance d'émission).

Avec le *BlocBallon*, construit sous la forme d'un gonflable (avec son potentiel politique comme objet de contestation) allié à de l'électronique embarquée (avec son potentiel d'obfuscation), deux types d'interaction émergent. D'une part, il génère une interaction passive amenée par le fonctionnement du dispositif électronique intégré, qui protège les personnes en présence sans même qu'ils aient besoin d'en avoir conscience. D'une autre part, il induit une interaction active lorsqu'il est porté par les manifestants tout en endossant un rôle symbolique de lutte contre les IMSI catchers. Dans ce cas d'étude spécifique, nous avons exploré une trajectoire possible, mais d'autres pourraient être tirées en identifiant d'autres cadres spécifiques en prenant par exemple les cas particuliers de l'usage de l'IMSI catcher dans l'espionnage industriel, du contrôle aux frontières ou encore dans le renseignement carcéral. De la même manière, cette méthodologie pourrait être appliquée à d'autres objets dans le champ de la surveillance tel que les algorithmes de reconnaissance faciale ou de reconnaissance de la démarche[63] par exemple pour en saisir l'importance dans la vidéosurveillance.

63 Qui reconnaît les individus à leur manière de marcher.

Fig. 59. Félicien Goguey. *BlocBalloon* poster #1. 2019. Design graphique & illustration: Salômé Guillemin.

BLOC BALLOON

An obfuscation tool to protest against cellphone surveillance

Throughout the 2010's, several newspapers related occurrences of weird interactions with mobile phones in demonstrations, as well as appearances of uncommon apparatus onboard emergency vehicles. These occurrences are symptomatic of the use of IMSI catchers (also known as Stingray in North America): a device used by law enforcement, the military and spies, among others, for cellphone surveillance. Organizations defending the right to privacy, such as EFF and Privacy International, underline the intrusive and undetectable character of this device as well as its dragnet nature making it a controversial object, reinforced by the vagueness surrounding its use. The legitimacy of these devices is often contested or at least questioned.

IMSI catchers can be found in multiple shapes, from hand-carried suitcases to fake light poles. Some versions are embedded in vehicles (cars, drones), turning them in highly mobile citywide surveillance devices. For a long time illegal, the use of such devices has been legalized in post-terror context laws, including in France (2015) and Switzerland (2016). An IMSI catcher mimics the activity of a cell tower to intercept your IMSI and your communications. The IMSI – standing for International Mobile Subscriber Identity – is a unique ID associated to your SIM card. When law enforcement operates an IMSI catcher in a given geographic area (e.g. a demonstration) and obtains relevant IMSIs, they can then use the legal process to obtain individuals' (e.g. protesters') identity.

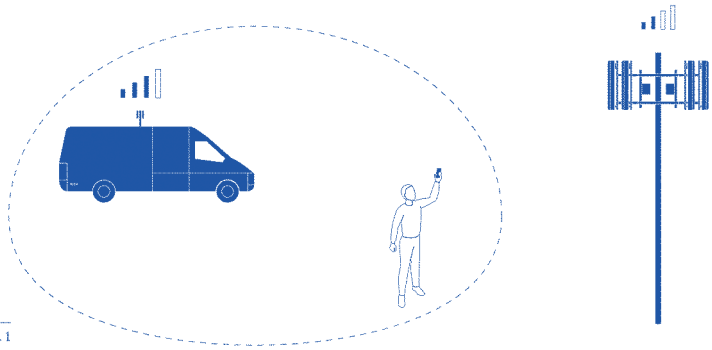


Fig. 1

In GSM networks (the protocol used for 2G communications), phones connect to the base station emitting with the strongest signal strength. IMSI catchers exploit this weakness to "catch" (i.e. record) IMSIs : while your phone thinks it's associated to a legitimate network, it's actually connected to the rogue device (Fig.1). This is the most basic interaction of an IMSI catcher, but some models can launch more sophisticated attacks that can lead to communication interception. Moreover, more advanced techniques can be involved to convince a phone to use 2G instead of the more secure 3G or 4G (i.e. with the use of jammers).

In order to demonstrate against phone targeting, we designed BlocBalloon, a disobedient object relying on electronic obfuscation and taking the form of an inflatable. This inflatable, designed to be carried during demonstration offers a collective mean of defense and protestation against GSM surveillance. It obfuscates IMSI catchers by masking protesters' IMSI and emitting fake or anonymous ones in a given area. The BlocBalloon relies on the same principles and flaws exploited by rogue cell towers to protect protesters from cellphone surveillance. When staying within its range, protesters' phones are associated with the BlocBalloon, thus defeating law enforcement devices (Fig.2).

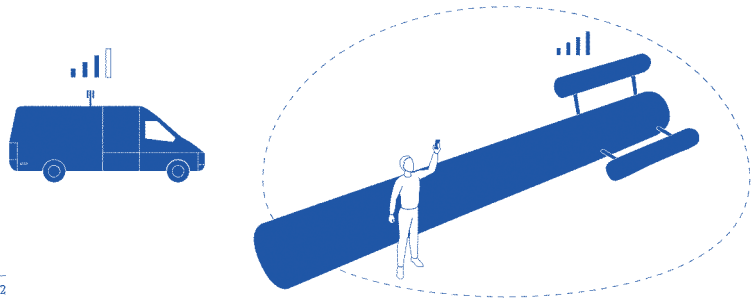


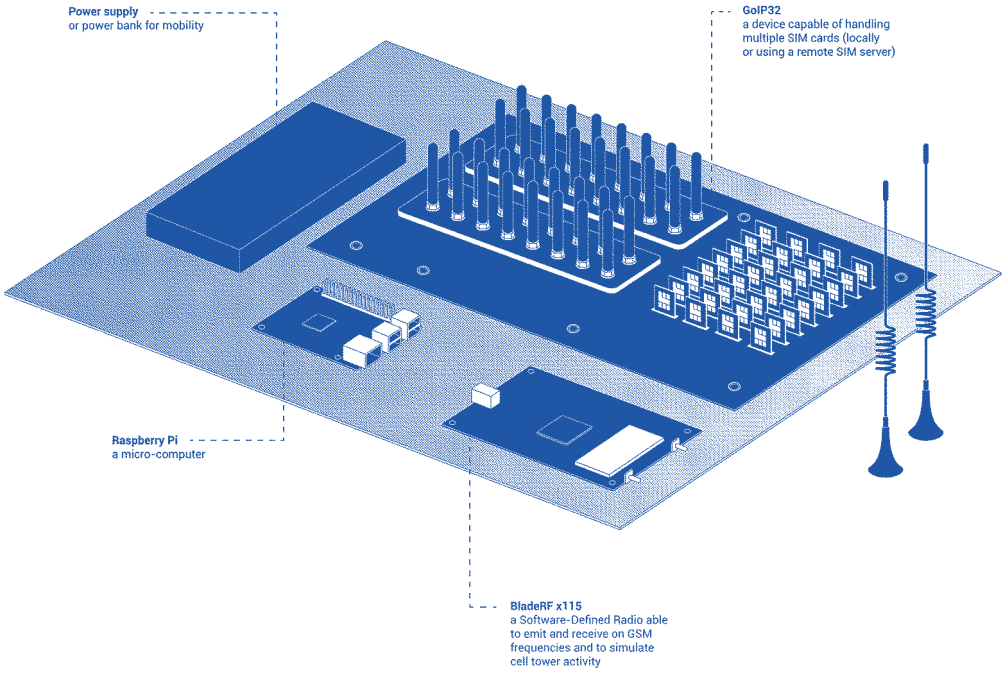
Fig. 2

Fig.60. Félicien Goguey. *BlocBalloon* poster #2. 2019. Design graphique & illustration: Salômé Guillemin.

#3

BLOC BALLOON

An obfuscation tool to protest against cellphone surveillance



The obfuscation process is achieved through the following steps :

- prior to the demonstration, the operator needs to generate IMSIs and burn them to SIM cards: this can be done with programmable SIM cards; alternatively, the operator can use anonymous SIM card ("pay-as-you-go" SIM cards, available in some countries);
- the IMSI catcher (or Cell Site Simulator) embedded in the BlocBalloon "catches" the phones of protesters in its scope. In this way the phones caught cannot be caught by another IMSI catcher (i.e. a law enforcement one);
- each time a protester's IMSI is caught, the device handling the programmed SIM cards substitutes it with an anonymous or a fake one;
- once they've become "invisible" on the network, the protesters receive a message informing them that they are under the protection of the BlocBalloon.

Fig.61. Félicien Goguey. *BlocBalloon* poster #3. 2019. Design graphique & illustration: Salômé Guillemin.

7
Recherche par le design III : Vers le design fiction

Comme nous l'avons vu dans le chapitre précédent, les prototypes spéculatifs, qu'ils soient fonctionnels ou non, permettent de déployer un espace discursif et de pressentir des trajectoires. Pour étendre cet espace et montrer que ces prototypes s'inscrivent dans un environnement sur lequel ils ont des conséquences, il est possible de construire des narrations dans lesquelles se déploient des designs fictions. En effet, ces narrations — ou scénarios — mettent en scène les objets produits et permettent d'étendre la discussion et le discours à tout un monde dans lequel il est possible de tester des hypothèses et d'explorer d'autres conséquences. Les scénarios constituent un aboutissement en ce sens qu'ils sont des objets finis, qui peuvent exister sous la forme de texte, de storyboard ou de vidéo comme nous le verrons plus tard ; mais aussi une ouverture puisqu'ils permettent d'explorer les effets sur un milieu plus large. Ils constituent ainsi une série d'hypothèses de design, de synthèses, d'avertissements et de récits mettant en scène les risques et les enjeux de manière lisible et compréhensible.

Ainsi, dit autrement, si l'on reprend le cadre théorique simondonien employé dans cette thèse, il est possible d'explorer le degré de concrétisation d'un objet technique en le formalisant dans un prototype spéculatif. Les scénarios, en mettant en scène ces objets, permettent d'illustrer certaines conséquences qu'ils peuvent avoir sur leur environnement — ou pour reprendre les mots de Simondon, sur leur milieu associé. Ces design fictions permettent donc d'émettre des hypothèses de design sur les manières dont les objets techniques concrétisés peuvent ou non modifier leur milieu associé. Je décrirai dans un premier temps la méthodologie employée pour construire l'ensemble des scénarios, puis je détaillerai leur construction pour chacun des scénarios.

7.1 Construction des scénarios

Les scénarios qui suivent ont été construits selon trois axes qui une fois assemblés par deux ont donné trois matrices. Chaque scénario trouve sa place dans une de ces matrices. Les axes ont été obtenus en observant des signaux faibles c'est-à-dire des actualités ou des faits divers qui laissent présager une tendance. Cette démarche est basée sur l'« analyse morphologique » que Véronique Lamblin, directrice d'études prospectives et stratégiques à Futuribles[64], définit comme suit :

> « L'analyse morphologique permet d'explorer les futurs possibles d'un système, à partir de la combinaison des hypothèses associées à ses variables ou ses composantes. À l'origine utilisée en innovation technologique, cette méthode se prête aussi à la construction de scénarios prospectifs. La trame d'un scénario sera alors une combinaison des hypothèses sur l'évolution des variables du système ;

64 <https://www.futuribles.com/fr/> consulté le 15.02.2022

chaque scénario représentant un jeu d'hypothèses différent. Stimulante pour l'imagination, l'analyse morphologique permet un balayage systématique et transparent du champ des possibles. »[65]

Ainsi, les trois axes choisis trouvent leur origine dans des composantes technologiques (Axe 1), politiques (Axe 2) et sociétales (Axe 3) qui trouvent chacune leur pertinence dans l'étude de l'IMSI catcher comme objet de la surveillance.

La date de 2025 a été choisie pour faire en sorte que les tendances qui ont été retenues pour la construction des axes aient le temps de se réaliser dans ce futur relativement proche, cela permet de conserver une certaine vraisemblance quant aux développements possibles et d'ancrer leurs origines dans des faits réels et présents. Je présenterai ainsi ces axes et les matrices obtenues en les assemblant.

Axe 1 : 2G/5G

L'axe 1 est construit sur l'abandon progressif de la 2G et l'arrivée de la 5G. En effet, en France et en Suisse on assiste à un démantèlement progressif de la 2G et à l'attribution de nouvelles bandes de fréquences aux opérateurs pour le déploiement de la 5G[66]. Cet axe concerne directement les IMSI catchers, puisque comme nous l'avons vu ceux-ci fonctionnent principalement sur la 2G ; il permet de poser plus généralement la question du devenir des dispositifs qui fonctionnent toujours sur la cette génération et du futur possible des bandes de fréquences libérées. En outre, il permet de soulever la possibilité d'une surveillance accrue par la conception d'autres dispositifs qui tirerait parti de la 5G ; en effet, si cette nouvelle technologie promet une connectivité et un débit toujours plus élevés elle apporte surtout de nombreuses évolutions pour les objets connectés et les systèmes autonomes. Enfin, cet axe permet d'évoquer certaines craintes sanitaires suscitées par l'arrivée de la 5G.

Axe 2 : politique sécuritaire/politique libertaire

L'axe 2 se dessine entre une volonté politique sécuritaire ou de contrôle et une volonté politique libertaire, avec moins d'outils de contrôle. En effet, depuis plusieurs années, dans un contexte de lutte anti-terroriste, de lutte anti-criminelle ou de crise sanitaire, les gouvernements adoptent le plus souvent une politique qui met plus d'outils de surveillance et de contrôle à disposition des autorités

65 <https://www.futuribles.com/fr/groupes/prospective-and-strategic-foresight-toolbox/document/lanalyse-morphologique/> consulté le 15.02.2022

66 <https://www.rts.ch/play/tv/19h30/video/la-2g-va-disparatre-des-antennes-telephoniques-suisses-dici-2021--cette-technologie-a-permis-lacces-a-la-telephonie-mobile-?urn=urn:rts:video:11138320> consulté le 15.02.2022

concernées. Ces politiques sont souvent mises en place en réponse à un contexte de crise. Ainsi, nous avons pu particulièrement constater de telles tendances pendant la pandémie de COVID-19. Ainsi en Suisse, au début du confinement il a été envisagé d'utiliser les données téléphoniques privées des citoyens pour éviter les rassemblements[67]. À cette politique sécuritaire viennent s'opposer des mouvements libertaires qui prônent le respect des libertés individuelles. Cet axe permet ainsi d'explorer les éventuelles conséquences dans l'application d'une politique sécuritaire qui demande toujours plus d'outils de contrôle ou d'une politique libertaire qui reposerait plutôt sur une responsabilisation individuelle et un respect strict des libertés.

Axe 3 : population prosurveillance/réticence de la population

L'axe 3 s'articule sur le degré de confiance et sur le degré de défiance de la population envers les systèmes de surveillances et les personnes qui les utilisent. Pour prendre un exemple de degré de confiance élevé, on peut citer la votation en Suisse de la Loi fédérale sur le renseignement (LRens) du 25 septembre 2016 adoptée à 65,5 % (avec une participation de 42,94 % des électeurs), qui accorde plus de moyens de surveillance aux autorités dans la lutte contre le terrorisme et la criminalité au détriment de certaines libertés individuelles. En opposition, des groupes activistes, mais aussi des associations de défenses des libertés présentent un degré de défiance fort qu'ils expriment à travers des actions de prévention ou des manifestations. Cet axe permet aussi de montrer l'existence de groupes de surveillance qui se constituent en milices citoyennes comme c'est le cas des *border watchers*[68] : des volontaires américains qui échangent sur un groupe Facebook à propos des flux migratoires à partir d'images vidéo de la frontière États Unis-Mexique.

Combinaisons

En combinant à chaque fois deux des trois axes énoncés précédemment, on obtient trois combinaisons possibles, à savoir :

- Matrice A : 2G/5G — politique sécuritaire/politique libertaire,
- Matrice B : 2G/5G — population prosurveillance/réticence de la population,
- Matrice C : politique sécuritaire/politique libertaire — population prosurveillance/réticence de la population.

67 <https://www.letemps.ch/economie/swisscom-aidera-confederation-detecter-attroupements-via-telephones> consulté le 15.02.2022

68 <http://www.virtualwatchers.de/> consulté le 15.02.2022

En explorant les différentes zones dans ces combinaisons et les tensions entre certains axes, il est possible d'y faire émerger des scénarios.

Alun Rhydderch, directeur de Soif-Horizons et fondateur de la SOIF (School of International Futures), présente cette démarche comme « *The 2x2 Matrix Technique* », soit la technique de matrice 2x2 ; d'après lui, cette technique de génération de scénario consiste à constituer en paire les facteurs de la plus haute importance et qui présente la plus grosse incertitude pour le sujet étudié et permet ainsi d'obtenir des matrices 2x2 qui forment la base pour des scénarios possibles. Cette approche est souvent utilisée pour tester des stratégies à moyen ou long terme parce qu'elle assure que la direction de la stratégie est robuste dans une palette d'environnements.[69]

7.2 Scénarios prospectifs

Scénario 1 : La 2G, domaine public

2025, canton de Genève, Suisse.

Comme dans le reste du pays, depuis 2020, les grands groupes de télécommunication se font la course pour se voir attribuer les meilleures bandes de fréquence pour l'exploitation de la 5G. Toutefois, ils rencontrent une forte opposition des militants 5G, d'autant plus sur le canton de Genève. En effet, avec la vague verte post-covid, qui a fait suite à l'appel du 4 mai 2020, le Grand Conseil présente une majorité de gauche écologique. Le réseau 2G avait déjà été en partie démantelé avant ce renversement politique « pour faire de la place à la 5G », tout en maintenant les réseaux 3G et 4G. Face au risque sanitaire et à la contre-initiative populaire « anti-5G » qui a fait suite au moratoire, le Grand Conseil décide de stopper le développement de la 5G et d'attribuer les fréquences 2G désormais libres (autour de 900 MHz) au domaine public.

Ainsi, on voit apparaître un réseau 2G basé sur un protocole GSM amélioré et *open source* qui est l'affaire de tout.e.s. En effet, le protocole GSM repose sur une technologie peu onéreuse et relativement facile à déployer. Ce réseau est composé d'une multitude de cell-sites privés ou publics qui émettent à faible puissance (et donc faible portée), ils nécessitent un maillage serré. On voit ainsi apparaître une multitude d'entités qui donne accès au réseau (comme on avait pu l'observer au début d'Internet). Néanmoins, devant l'abandon de l'État des techniques de surveillance du réseau téléphonique mobile, certains citoyens ont

69 <https://www.futuribles.com/fr/groupes/prospective-and-strategic-foresight-toolbox/document/scenario-building-the-2x2-matrix-technique/> consulté le 15.02.2022

un sentiment d'insécurité fort et s'inquiètent de la non-possibilité de surveillance et de traçage des citoyens au sein de ces réseaux ouverts. Ainsi, certains opposants s'organisent en milices citoyennes de surveillance (comme l'EMS : *Electro-Magnetic Swissveillance*), basés sur le modèle « *neighborhood watchers* », ils.elles prônent une surveillance décentralisée et symétrique, où chacun.e.s des citoyen.ne.s peut utiliser son propre IMSI catcher afin de surveiller son.sa voisin.e. C'est l'avènement de l'IMSI catcher personnel, objet vigilant et DIY ; il est accessible à toute personne ayant un minimum de connaissance du protocole. Pour les néophytes, il existe des workshops, à l'issue desquels ils peuvent repartir avec leur propre IMSI catcher. Dans un premier temps, certains opposants à ce qu'ils appellent eux-mêmes « l'extrémisme vert » décident de s'équiper, afin de surveiller des communautés entières. Puis, des groupes anti-immigration récupèrent ce dispositif et se postent à des points stratégiques des frontières pour repérer les migrants à la manière des volontaires américains qui surveillent la frontière avec le Mexique à l'aide de caméras de surveillance.

Ce scénario peut donner plusieurs développements à explorer ; par exemple la constitution d'une opposition aux milices citoyennes de surveillance, les potentiels outils mis à disposition par les milices citoyennes pour réaliser son propre IMSI catcher, les relations avec la France voisine (scénario 3), la réaction des groupes de télécommunication.

Construction du scénario 1

Le scénario 1 est issu de la matrice A. Il explore un retournement de situation dans lequel la 2G est maintenue et tombe dans le domaine public, la 5G n'est pas développée. Dans cet élan « *open source* » et libertaire, le gouvernement abandonne les outils de surveillance. Il apparait dans un contexte post-covid et s'appuie sur l'Appel du 4 mai 2020 pour un redémarrage « humaniste, local et durable »[70] et permet d'explorer comment les citoyens réagissent dans cet État où la surveillance existe peu.

Scénario 2 : Le consensus 2G/5G

2025, France et Suisse.

La 5G, poussée par les lobbies, permet des communications plus rapides et plus sécurisées surtout pour les objets connectés et les véhicules autonomes. Toutefois, devant l'inquiétude sanitaire et écologique qu'elle suscite, les citoyens exigent que des études indépendantes sur sa nocivité soient menées. En attendant les résultats de ces études, le développement de la 5G est suspendu et les

70 <https://www.rts.ch/info/suisse/11295271-lappel-du-4-mai-pour-un-redemarrage-humaniste-local-et-durable.html> consulté le 15.02.2022

infrastructures des générations précédentes (2G, 3G et 4G) sont conservées.

Cette co-existence des protocoles permet d'utiliser des IMSI catchers, ainsi que de nouveaux moyens de surveillance. C'est d'ailleurs devant le recours quasi-systématique aux IMSI catchers lors des manifestations (Black Lives Matter, Extinction Rebellion) notamment embarqués sur des véhicules (voitures et avions), que des groupes de chercheurs et des réseaux d'activistes s'organisent pour lutter contre cette utilisation abusive : ils déploient des outils de mesure de cette surveillance et réclament plus de transparence quant à ces recours systématiques. Un de ces outils, SeaGlass, basé sur un assemblage de différents composants électroniques et informatiques, permet de détecter des anomalies dans le réseau cellulaire en toute légalité, et par extension, la présence d'IMSI catchers dans une zone donnée. Il est d'abord porté par des volontaires dans leur sac à dos ou leur véhicule personnel. Puis grâce à l'accord inédit de certaines compagnies de transports publics, l'outil a pu être installé dans des bus et des trams.

Cet outil est ensuite amélioré et miniaturisé pour devenir un *wearable*, que chacun.e peut porter dans l'espace public et notamment dans les manifestations, afin d'être (1) averti en cas de présence d'un IMSI catcher et (2) contribuer à la cartographie de leur utilisation. Par extension, les porteurs du *wearable* font émerger sur la carte l'utilisation abondante des IMSI catchers aux abords des frontières et révèlent leur rôle dans le contrôle de l'immigration. Cette carte, véritable preuve de l'utilisation abusive de l'IMSI catcher et des dérives qui l'accompagnent, affectera l'opinion publique et permettra de rétablir un débat public autour cet objet de surveillance trop longtemps ignoré.

Ce scénario peut donner plusieurs développements à explorer ; par exemple les nouveaux moyens de surveillance de la 5G, le design du *wearable*, les effets de celui-ci et de la carte sur l'opinion publique, dans l'utilisation de l'IMSI catcher dans les manifestations et dans le contrôle des frontières.

Construction du scénario 2

Le scénario 2 est issu de la matrice B. Il explore un consensus dans lequel la 2G et la 5G co-existent, et dans lequel la population présente un degré de défiance assez fort envers les autorités et leurs outils de surveillance. Cette tendance à la défiance repose sur des outils existants actuellement comme SeaGlass[71] développé par une équipe de chercheurs à l'Université de Washington ; ainsi que sur des signaux faibles que j'ai pu observer au moment de la construction du scénario, à savoir : l'utilisation d'avions pour survoler et surveiller les manifestations Black Lives Matter de 2020[72], on peut supposer que ces appareils embarquaient des

71 <https://seaglass.cs.washington.edu/> consulté le 15.02.2022

72 <https://edition.cnn.com/2020/06/11/politics/spy-planes-george-floyd-protests/index.html> consulté le 15.02.2022

IMSI catchers ; cet appel à projets du ministère des Armées[73] qui vise à intégrer sur des drones une charge utile qui « doit pouvoir détecter, localiser, identifier voire interagir ou bloquer des émetteurs de télécommunication » ; cet article de presse[74] qui divulgue que la Direction nationale du renseignement et des enquêtes douanières a fait l'acquisition d'IMSI catchers alors que leur utilisation était encore illégale ; cet autre article de presse[75] qui dévoile que des agences de l'immigration américaine utilisent des « dispositifs invasifs visant les téléphones portables ».

Scénario 3 : Un totalitarisme sécuritaire

2025, France.

Dans un contexte ultra-sécuritaire post-attaques terroristes et post-pandémie, après les lois sur le renseignement de 2015 et sur le traçage des contacts sociaux de 2020 passées pendant l'état d'urgence, l'État dispose d'un arsenal sécuritaire qui échappe au pouvoir judiciaire. Parmi cet arsenal, le pouvoir exécutif s'appuie sur le déploiement d'IMSI catchers fixes qui permettent à tout moment de repérer un individu sur tout le territoire français, sans faire appel aux opérateurs mobiles que ce soit dans l'espace public ou dans les espaces privés, ce qui lui confère une grande marge de manœuvre pour la détection et l'interception d'individus. Ce réseau de *cell-site simulators* à échelle nationale permettent un traçage en temps réel et extrêmement précis de la population française : dans cet état policier, l'anonymat n'est plus possible. On voit ainsi apparaître une asymétrie totale : l'État impose une surveillance omniprésente devant laquelle les citoyens ne peuvent quasiment pas agir. Cette surveillance constante et totale mène ainsi une autocensure extrême : se sachant surveillés les citoyens n'osent plus échanger.

Dans un premier temps, certains mouvements de résistance sont apparus, soutenus par des associations de défense des libertés individuelles, comme la Quadrature du Net. On a ainsi vu de nombreuses manifestations, notamment avec des gonflables d'obfuscation appelés *BlocBalloons*, symboles forts de la protestation. Puis, devant la répréhension de plus en plus forte, certains groupes militants ont commencé à détruire les IMSI catchers (comme ce fût le cas pour les radars routiers à leur apparition dans les années 2000). Certains opposants se déplacent constamment avec des *jammers* (notamment dissimulés dans des parapluies)

73 <https://www.defense.gouv.fr/aid/appels-a-projets/appel-a-projets-pour-une-mini-charge-utile-d-appui-electronique-sur-drones> consulté le 15.02.2022

74 <https://www.nouvelobs.com/rue89/rue89-police-justice/20150521.RUE9157/c-est-illegal-tant-pis-les-douanes-ont-achete-des-imsi-catchers.html> consulté le 15.02.2022

75 <https://www.aclu.org/news/immigrants-rights/ice-records-confirm-that-immigration-enforcement-agencies-are-using-invasive-cell-phone-surveillance-devices/> consulté le 15.02.2022

pour passer sous le radar : l'État riposte en déployant des *jammers-detectors*. Néanmoins, la traçabilité étant perçue par la majorité des citoyens comme un acte de civisme, les personnes qui la refusent se marginalisent, il devient de plus en plus difficile pour celles-ci de trouver un travail, un logement, d'accéder à des lieux publics ou encore de toucher des prestations sociales. En effet, pour accéder à ces droits, il est nécessaire de posséder un contrat de téléphonie mobile ; de plus, les personnes détentrices d'un *jammer* sont fichées dans un registre national.

Ce scénario peut donner plusieurs développements à explorer ; par exemple les effets sur les libertés d'expression et de mouvement ou le design d'objets désobéissants par les opposants pour continuer à passer sous le radar.

Construction du scénario 3

Le scénario 3 est issu de la matrice C, il se situe à l'extrême de l'axe de la politique sécuritaire et explore les tensions qui existent avec le degré de confiance ou de défiance de la population.

Un exemple de mise en forme

J'ai fait le choix d'illustrer le scénario 2 de manière plus approfondie pour montrer comment il pourrait apparaitre dans un contexte de groupe de discussion. J'ai choisi pour cela la vidéo ; c'est une forme de recherche par le design pour laquelle le choix des images et du son ont été faits afin de coller à une esthétique complotiste que l'on rencontre régulièrement sur YouTube ou Facebook. Ainsi elle est majoritairement constituée de captures d'écran d'articles de presse en ligne, de vidéos de manifestations et de captures vidéo de Google Earth. La voix off a été obtenue à l'aide d'un outil de génération de voix en ligne.

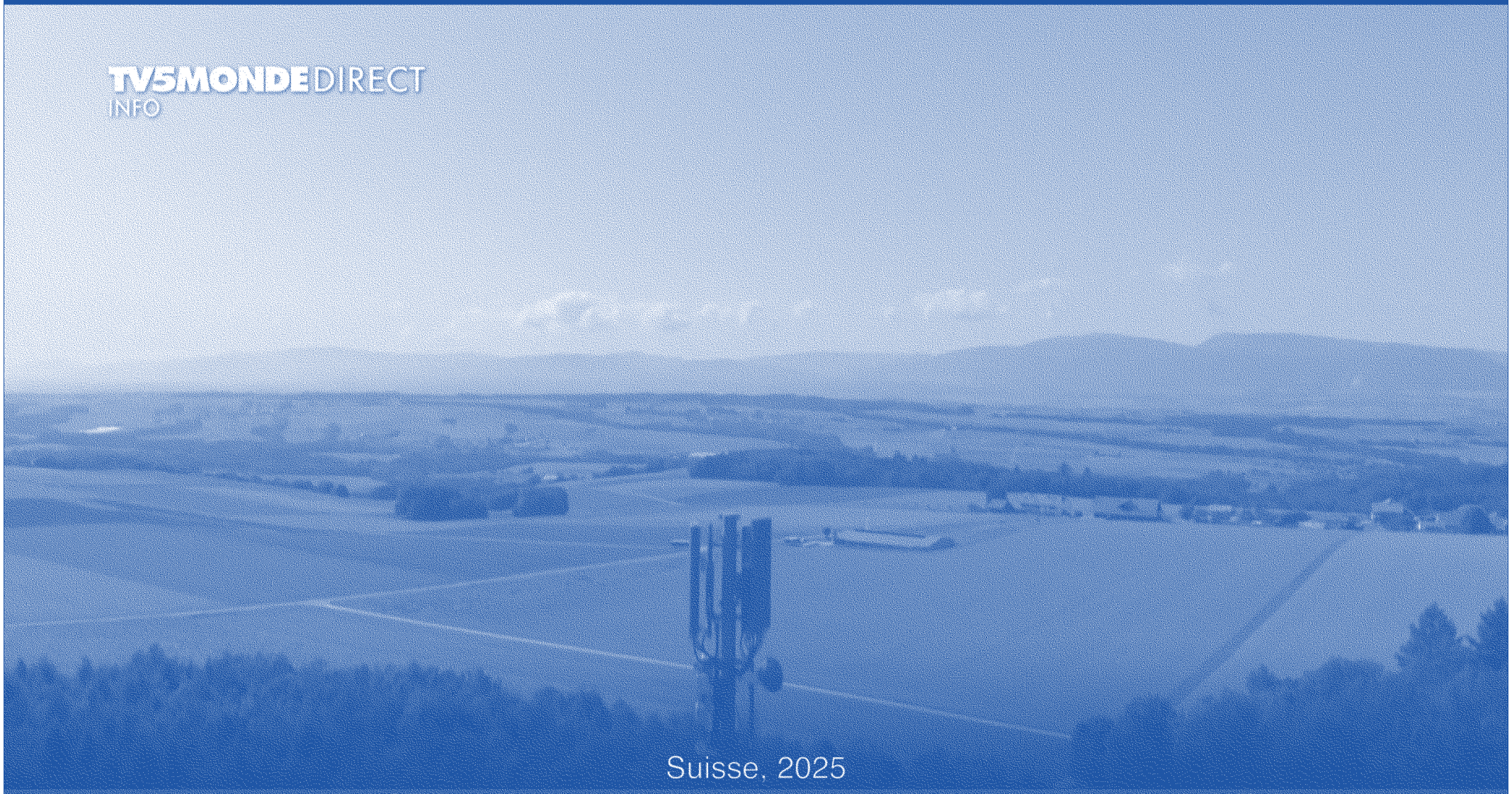
La vidéo a été mise en ligne sur la chaine YouTube *stop_gsm_surveillance*[76] le 26 novembre 2020 puis retirée par YouTube dans les semaines suivantes sans aucune notification[77], elle est téléchargeable depuis mon site internet à l'adresse suivante : <https://felicien.io/files/stop_gsm_surveillance.mov> consulté le 15.02.2022. Les images présentées à la suite de ce chapitre en sont extraites (pp.188-205).

Cette réalisation vidéo produite en fin de thèse permet de présenter de manière synthétique certains enseignements, certaines trajectoires et certaines des connaissances produites ici dans un objet fini. C'est une manière de valoriser

76 <https://www.youtube.com/channel/UCLGSIPl5a2sPCR4xHmPJkrw/featured>

77 Ce pourrait être une conséquence de l'utilisation d'un algorithme de modération automatique par la plateforme comme décrit dans cet article du Monde du 26 août 2020. <https://www.lemonde.fr/pixels/article/2020/08/26/youtube-a-double-la-suppression-de-videos-durant-la-pandemie_6049981_4408996.html> consulté le 15.02.2022.

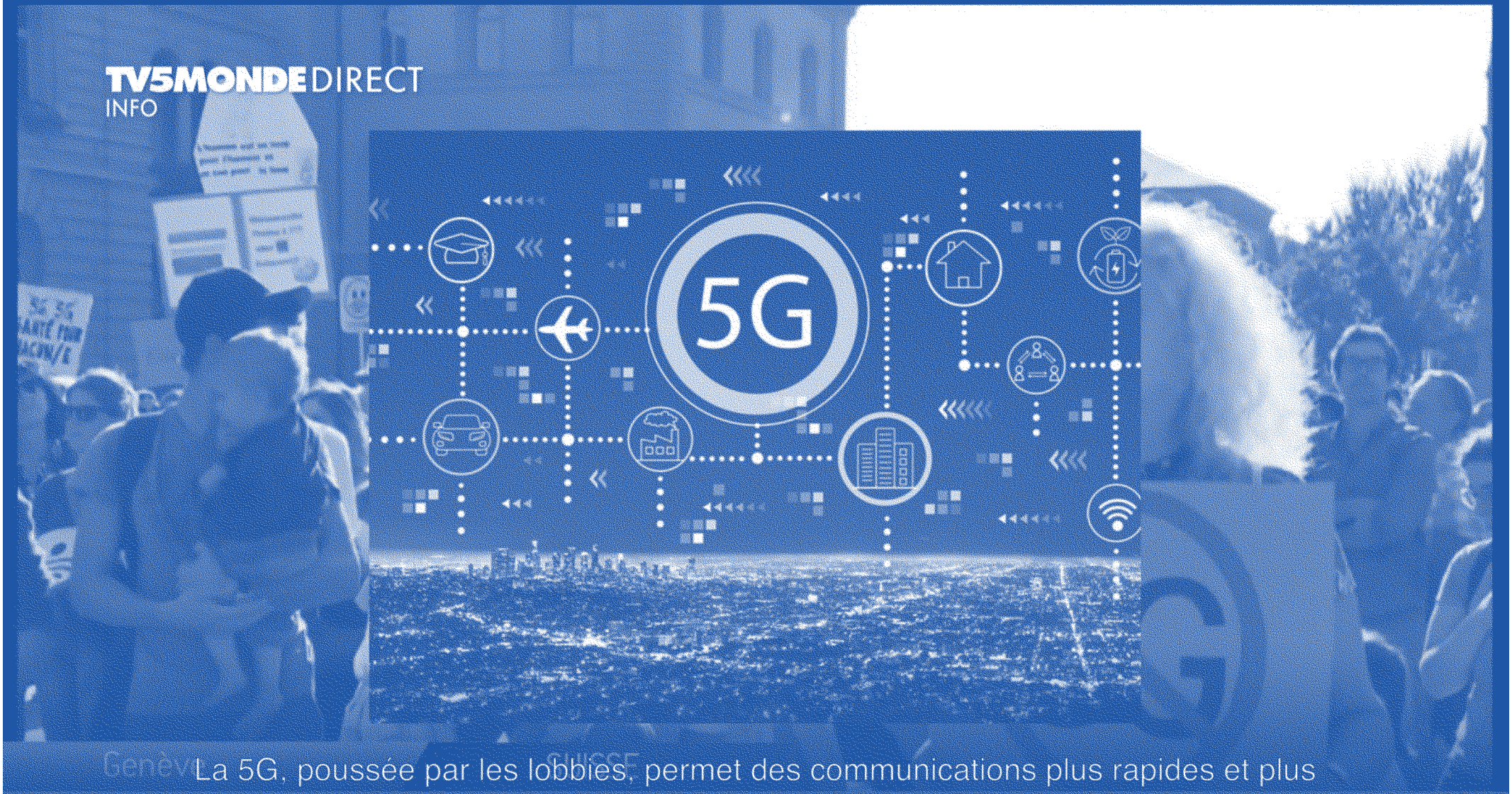
la thèse d'une part : on peut imaginer sa présence dans une exposition future qui présenterait les résultats de cette recherche d'une autre manière que par le format académique ; et c'est un outil discursif d'autre part. En effet, elle permet d'illustrer la transversalité des champs abordés ici par l'image (ce qui est parfois difficile à faire ressortir dans le texte) et permet de ce fait d'animer des discussions sur des questions transversales qui apparaissent tout au long de la thèse auprès d'un public non-averti. Il est ainsi possible d'aborder de manière plus large les grandes questions et les enjeux de la surveillance, notamment le rapport du citoyen à celle-ci et sa responsabilité à s'emparer du phénomène pour en souligner la préoccupation politique que celle-ci représente. Enfin, il serait possible sur le même modèle d'étendre le discours à d'autres formes de surveillance comme l'utilisation de la reconnaissance faciale dans le vidéo-surveillance et dans d'autres sphères du réseau comme le maillage de câbles optiques d'Internet.



TV5MONDE DIRECT
INFO

Suisse, 2025

© TV5 LE MONDE EN FRANÇAIS



La 5G, poussée par les lobbies, permet des communications plus rapides et plus sécurisées surtout pour les objets connectés et les véhicules autonomes.

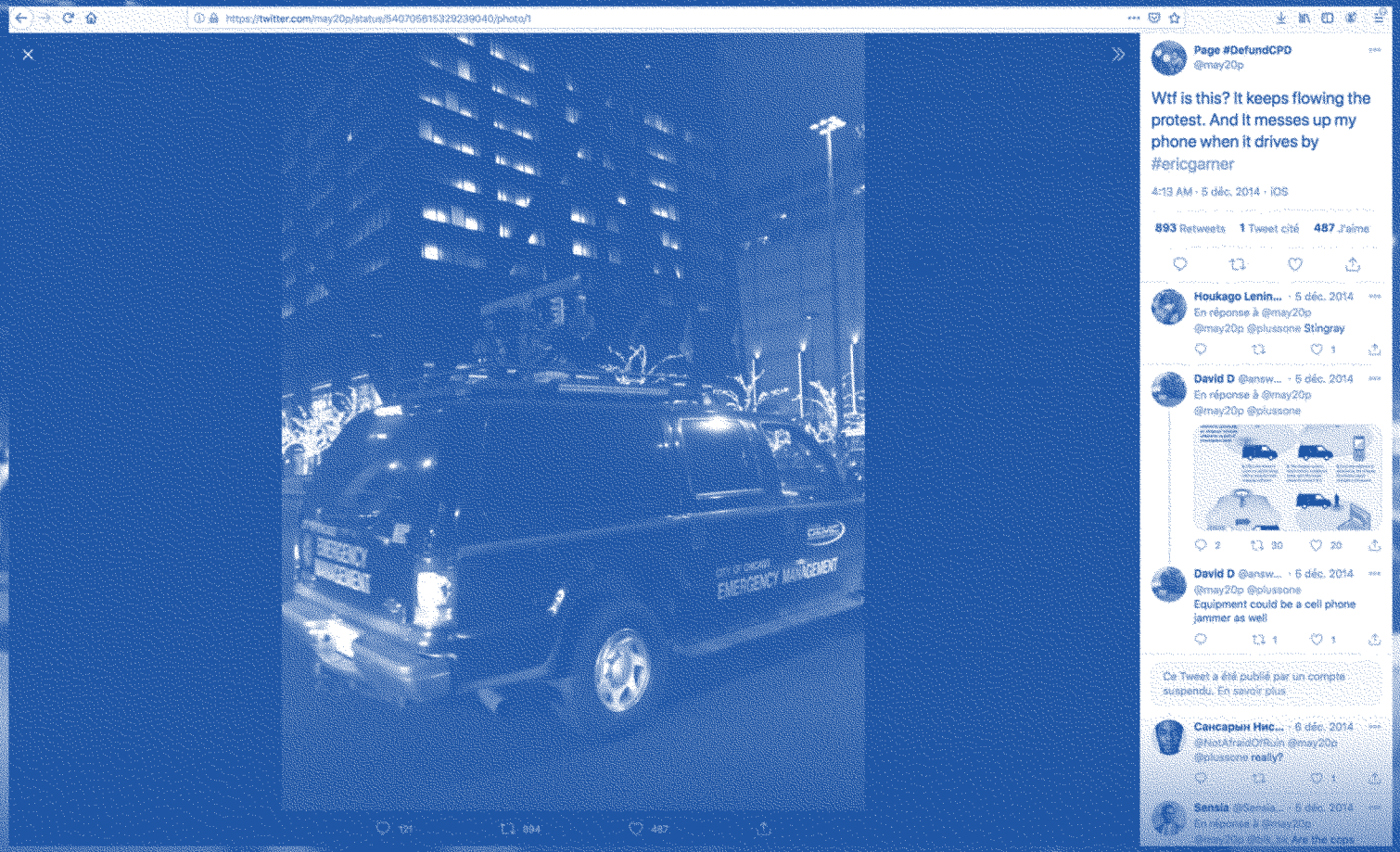
Toutefois, devant l'inquiétude sanitaire et écologique qu'elle suscite, les citoyens exigent que des études indépendantes sur sa nocivité soit menées.

CAMILLE SELLEGER

En attendant les résultats de ces études, le développement de la 5G est suspendu et les infrastructures des générations précédentes (2G, 3G et 4G) sont conservées.

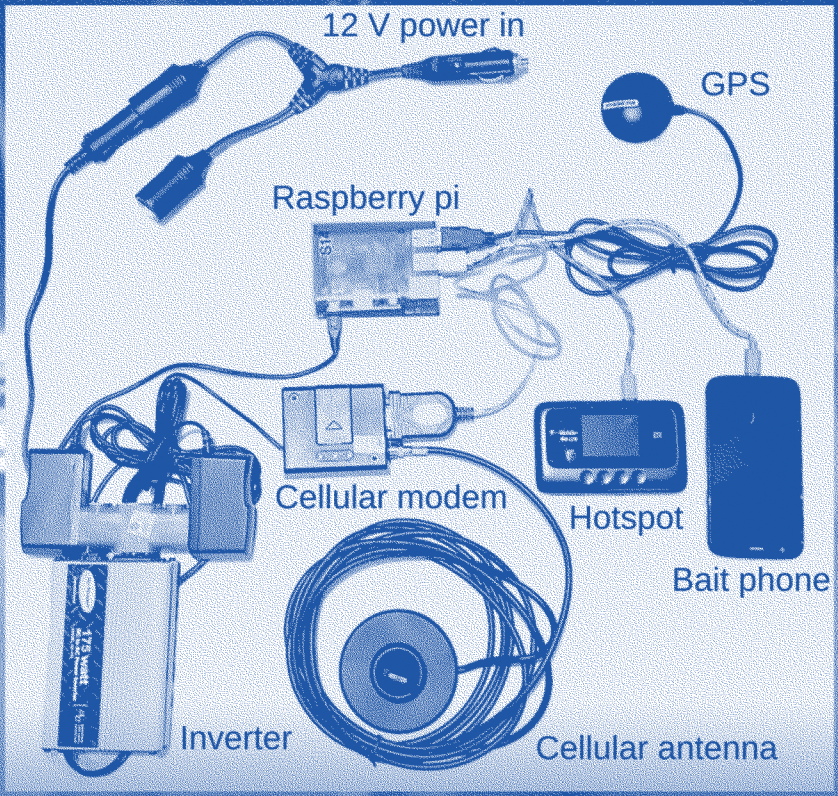
Cette coexistence des protocoles permet d'utiliser des IMSI catchers,
ainsi que de nouveaux moyens de surveillance.

C'est d'ailleurs devant le recours quasi-systématique aux IMSI catchers lors de manifestations notamment embarqués sur des véhicules (voitures et avions)



que des groupes de chercheurs et des réseaux d'activistes s'organisent pour lutter contre cette utilisation abusive :

ils déploient des outils de mesure de cette surveillance et réclament plus de transparence quant à ces recours systématiques.



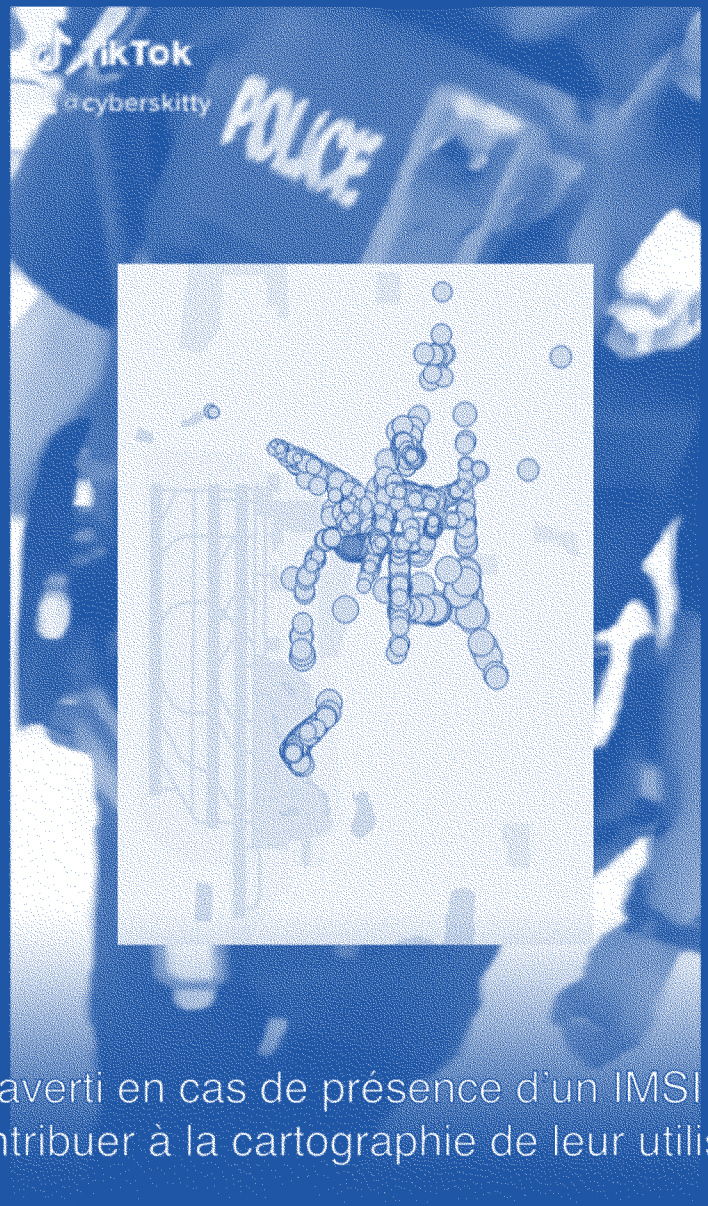
Un de ces outils, SeaGlass, basé sur un assemblage de différents composants électroniques et informatiques,

permet de détecter des anomalies dans le réseau cellulaire en toute légalité,
et par extension, la présence d'IMSI catchers dans une zone donnée.

Il est d'abord porté par des volontaires dans leur sac à dos ou leur véhicule personnel.

Puis, grâce à l'accord inédit de certaines compagnies de transports publics, l'outil a pu être installé dans des bus et des trams.

Cet outil est ensuite amélioré et miniaturisé pour devenir un wearable, que chacun.e peut porter dans l'espace public et notamment dans les manifestations,



afin d'être averti en cas de présence d'un IMSI catcher et de contribuer à la cartographie de leur utilisation.

Par extension, les porteurs du wearable font émerger sur la carte l'utilisation abondante des IMSI catchers aux abords des frontières

et révèlent leur rôle dans le contrôle de l'immigration.

Cette carte, véritable preuve de l'utilisation abusive de l'IMSI catcher
et des dérives qui l'accompagnent, affecte l'opinion publique

et permet de rétablir un débat public autour de cet objet de surveillance trop longtemps ignoré.

8
Discussion & conclusions

Nous avons pu voir au cours de cette thèse que l'IMSI catcher est un artefact au statut particulier, que j'ai qualifié d'agrégat technique comme un dispositif technique composite relevant d'un assemblage d'objets techniques. Malgré sa dénomination commune, il recouvre en réalité une multitude de modèles co-existants dans un même environnement, ce qui lui confère un statut particulier que j'ai pu déplier au moyen d'une recherche par le design. De plus, son utilisation soulève de nombreuses controverses notamment sociales et politiques ; en effet, son mode opératoire « coup de filet » intercepte toutes les communications dans une zone donnée et peut ainsi mettre en péril certaines libertés individuelles et collectives : le droit à la vie privée dans un premier temps, mais aussi les libertés d'expression et de se réunir notamment en conséquence de l'envoi de messages massif qui peuvent dissuader de se rendre à une manifestation par exemple. Ce même mode opératoire amène aussi des problématiques particulières qui en font un objet difficile à situer au sein des *surveillance studies* : il est difficile d'en définir le champ d'action, particulièrement en milieu urbain et plus encore s'il est embarqué sur des véhicules tels que des drones. Enfin, la recherche par le design à travers des méthodes spéculatives et prospectives a permis de concevoir et d'exposer des prototypes de contre-surveillance interrogeant sur la légitimité des usages de l'IMSI catcher ainsi que des scénarios questionnant les futurs possibles de cet objet de la surveillance. Au-delà de ce résumé, l'objectif de ce dernier chapitre est de discuter de manière transversale les différents aspects de l'IMSI catcher que j'ai abordés au cours de la thèse, je le fais en regard des notions centrales d'opacité et de transparence, tout en insistant sur les limites et les opportunités rencontrées.

Ainsi, sur la base de ces résultats, mais aussi en lien avec des considérations décrites dans mon cadre méthodologique et théorique, je présente dans cette conclusion trois axes de réflexion transversaux afin de souligner les apports de la thèse au-delà des objectifs initiaux : je reviens (1) sur le statut particulier de cet objet, j'aborde (2) son rapport à la spatialité et aux algorithmes ainsi que son régime de visibilité, je retrace (3) les différentes contre-mesures qu'il est possible d'entreprendre afin d'arriver à une possible contre-surveillance et à débattre de la légitimité des usages du dispositif, notamment autour de la transition 2G/5G et du futur potentiel de la surveillance du réseau téléphonique mobile.

8.1 Un objet au statut particulier

Nous avons pu le voir au cours de cette thèse, l'IMSI catcher est un objet au statut particulier. Tout d'abord, la façon dont on le nomme n'est pas la même selon le continent où l'on se trouve ou selon l'entreprise qui le produit (IMSI catcher, *Stingray*, *Dirtbox*). De plus, ces dénominations recouvrent en réalité une constellation d'objets aux formes extrêmement diverses (portables, transpor-

tables, embarqués par exemple) qui ont pourtant des fonctions d'usage proches ou identiques et qui reposent sur un principe de fonctionnement commun : exploiter les failles du protocole GSM afin d'intercepter les IMSI et certaines communications.

Toutefois, comme nous avons pu le voir dans « Recherche sur le design : Étude d'un objet confidentiel », il est difficile d'établir les lignées techniques de cet objet et ce à cause de plusieurs facteurs. D'une part, c'est un objet difficilement accessible, parce qu'il est la plupart du temps réservé aux autorités gouvernementales ou alors parce qu'il est extrêmement onéreux[78]. D'autre part, il co-existe une quantité innombrable (du fait de leur confidentialité) de modèles dont on ne connait pas nécessairement la date de conception et de production ; pour cette raison il n'est pas possible d'établir une chronologie fiable. Ceci est directement lié aux sources utilisées pour l'étude de l'objet : pour la plupart des catalogues ou des photos qui ont fait l'objet d'une fuite sur Internet et qui ne sont pas datés.

En ce sens, la recherche sur le design s'est heurtée sur une limite qui est l'approximation et la fiabilité discutable de certaines informations présentes dans les documents recueillis. Enfin, c'est un objet qui présente un degré de concrétisation très faible puisqu'il relève la plupart du temps d'un assemblage de composants facilement dissociables ; néanmoins, et malgré cette concrétisation peu avancée, il est possible de pressentir des degrés différents au sein de celle-ci et de deviner des embryons de lignées techniques ou de grandes tendances. Plus important encore, cette recherche sur le design a permis d'identifier les composants de l'IMSI catcher, à savoir : l'interface radio, l'antenne, l'amplificateur, l'alimentation et l'ordinateur ; c'est sur ce constat que j'ai pu amorcer une démarche de reconstitution à la manière des travaux réalisés par Egen et al. dans l'histoire des sciences (2012), Jentery Sayers dans les humanités numériques (2014, 2015) ou Thomas Thwaites dans le design (2011).

Pour autant, cette démarche de recherche sur le design s'est avérée pertinente pour désigner un ensemble de signaux faibles et de tendances qui a servi de base pour la spéculation de « présents alternatifs » et de « futurs possibles » (Auger, 2013). En effet, certains des aspects techniques de l'IMSI catcher (le fait qu'il ne fonctionne pas sur la 5G par exemple) ont permis de constituer des axes pour la construction des scénarios prospectifs. En outre, l'étude de la documentation visuelle des antennes présentes dans le corpus a permis d'orienter la conception des prototypes des chapitres 5 et 6.

De plus, devant le manque de sources est apparue la nécessité d'adopter une autre posture méthodologique. Sur la base de l'identification des différents composants

78 De quelques dizaines à plusieurs centaines de milliers de dollars américains selon les exemples du corpus.

et de la documentation de programmes logiciels *open source* (souvent issues de communautés de *hackers*), j'ai pu reconstituer trois prototypes d'IMSI catchers. Ainsi, en reprenant des méthodes habituellement appliquées à des objets historiques, mais en les appliquant cette fois-ci à un objet confidentiel il a été possible de confirmer l'hypothèse sur le caractère non-concret de l'IMSI catcher, en effet les trois reconstitutions sont basées sur l'assemblage de plusieurs composants (matériels et logiciels) indépendants les uns des autres et facilement séparables. En outre, cette démarche a permis d'identifier plusieurs « modes d'existence » de l'IMSI catcher, dans sa forme passive et dans sa forme active ; et en parallèle de cerner son fonctionnement et ses limites, ce qui a permis de lever une partie du flou — et peut-être une part de mythe — qui existe autour de cet objet. En effet, dans les articles de presse cités dans l'introduction et dans leurs commentaires, l'IMSI catcher était désigné comme un objet capable d'intercepter les appels et une autre action supposée était sa capacité siphonner la totalité des données contenues dans un téléphone. Le travail de reconstitution a permis de confirmer que l'IMSI catcher était en effet capable d'intercepter des appels — même si sa fonction première est de relever les identités des téléphones en présence ; toutefois, le mode opératoire de l'IMSI catcher n'indique pas que celui-ci soit capable d'intercepter autre chose que les communications GSM qui transitent sur le réseau, ce qui infirme l'hypothèse du siphonnage des données d'un téléphone[79]. Ce constat renvoie à la célèbre remarque de Gilbert Simondon, pour qui la méconnaissance de la machine est une cause d'aliénation (Simondon, 1958), et souligne l'importance d'un mode de connaissance des objets techniques, même s'ils sont abscons.

Ensuite, la production de ces trois reconstitutions a démontré qu'une méthodologie par la reconstitution permet de s'adresser à un objet complexe tel que l'IMSI catcher afin d'en faire d'autres utilisations. En effet, ces reconstitutions ont permis de constituer une base précieuse sous la forme boîte à outils : d'outils logiciels d'une part (différents programmes d'acquisition et de traitement des données du réseau téléphonique mobile) et d'outils matériels d'autre part (assemblage d'antennes et cartes radio différentes selon l'objectif visé). Ces outils sont autant de « briques de base » à assembler afin d'obtenir les productions suivantes : tout d'abord la performance audiovisuelle *900 MHz* et plus tard les objets de contestation. Ainsi les prototypes *MOTO* et *REAL* sont à la base de l'acquisition des données utilisées dans la performance *900 MHz*, ils ont ensuite servi d'outils d'audit pour la conception des objets de contestation. Le fonctionnement du *BlocBalloon* pour sa part repose principalement sur la reconstitution de l'IMSI catcher actif *BLADE*, lequel est directement intégré au gonflable.

79 Dans l'éventualité où de telles actions sont possibles, elles sont visiblement attribuées à tort à l'IMSI catcher et relèvent plutôt d'autres dispositifs potentiellement utilisés en conjonction avec l'IMSI catcher.

Ces différentes productions démontrent que la reconstitution est une première étape vers la réappropriation de l'objet technique par la rétro-ingénierie, le *critical making* (Hertz, 2012), le *critical unmaking* (Nova, Bloch, 2020) , et le « contre-faire » (Allard, 2015). Hertz défend par le *critical making* une vision de la recherche qui passe par le « faire » — *making* — en ce qu'elle peut compléter et étendre une réflexion critique sur la technologie et la société. Nova et Bloch voient dans le *critical unmaking* une manière d'acquérir de la connaissance à partir du démontage « officieux » et documenté par les réparateurs eux-mêmes d'objets technologiques. Allard propose un scénario dans lequel le citoyen s'opposerait au contexte actuel et resterait « maître dans le cadre d'un scénario socio-technique sécurisé qui ne peut profiter qu'à l'intelligence collective environnementale ». L'approche adoptée au cours de la thèse emprunte à chacune des notions précédentes.

La démarche de reconstitution adoptée ici va néanmoins au-delà du *unmaking* puisqu'elle s'appuie sur une forme de culture DIY et de hacking et qu'elle requiert que des conditions soient réunies. D'une part des conditions techniques, dans le cas de l'IMSI catcher c'est le fait qu'une partie du matériel utilisé était facilement accessible, peu onéreux et facilement détournable de leur usage premier ; et d'autre part des conditions sociales, notamment l'existence de communautés *open source* qui mettent à disposition du code logiciel et une documentation fournie afin de pouvoir exploiter le matériel précédemment cité. Enfin, il est possible d'émettre une condition culturelle, directement liée à ces communautés ouvertes qui prônent le DIY, qui est cette volonté de constamment s'approprier les technologies afin de dé-construire et questionner leurs usages — ce qui se rapproche de la démarche des ingénieurs critiques (Oliver, Savičić, Vasiliev, 2011).

De plus on peut rapprocher la démarche de reconstitution de la démarche du « contre-faire » (Allard, 2015), c'est-à-dire au sens de son autrice de faire autrement, et qui pose la question « dans quel monde voulons-nous être connectés ? ». En ce sens, s'atteler à la reconstitution de l'IMSI catcher permet de se le réapproprier (et d'une certaine manière de se réapproprier la nature des données qu'il intercepte) et de s'approcher ainsi d'une démarche citoyenne dans laquelle le « citoyen capteur [...] devrait être à la fois producteur et interprète de ses propres données ». Cette notion du contre-faire permet d'aborder une autre condition qui est liée au fait de faire ce genre de reconstitution pour acquérir, développer et transmettre des compétences techniques quant aux objets qui font l'infrastructure de notre quotidien ; en l'occurrence, au-delà du fonctionnement même de l'IMSI catcher, le travail de reconstitution a permis par extension de cerner le fonctionnement d'une antenne relais et du réseau téléphonique mobile dans son ensemble. Aussi, les pratiques de recherche-création convoquées dans ce contexte permettent non seulement de montrer, mais aussi d'ouvrir, de démonter et de refaire la boîte noire. C'est d'une part une démarche citoyenne qui permet

d'apporter une réflexion sur les objets qui nous entourent (et ce qu'ils soient visibles ou non) et à laquelle on pourrait ajouter une dimension participative (on pourrait ainsi imaginer des ateliers « fais-ton propre IMSI catcher ») ; et d'autre part une démarche qui s'inscrit dans une épistémologie du design et qui permet de montrer que sa conception ne repose pas uniquement sur des choix techniques, mais aussi politiques. Enfin, la démarche adoptée ici permet d'aller au-delà de l'ouverture de la boîte noire et de réappropriation citoyenne des données, en proposant des alternatives et des portes de sortie face à la surveillance comme nous le verrons plus bas.

Toutefois, il est nécessaire de rappeler certaines limites des objets reconstitués inhérentes au statut de l'IMSI catcher. D'une part, il n'a pas été possible de le tester en « conditions réelles », mais uniquement dans un milieu contrôlé, principalement pour des raisons légales, mais aussi à cause de limitations techniques. D'autre part, il est difficile d'évaluer l'efficacité des différents prototypes que j'ai produits en comparaison des IMSI catchers existants sur le marché commercial pour des raisons déjà citées plus haut. Néanmoins, cela a permis de mieux délimiter l'objet en gardant quelques réserves sur les capacités réelles des IMSI catchers commercialisés et les choix faits par leurs concepteurs. En ce sens, la reconstitution a elle seule n'a pas permis de découvrir la vision des concepteurs constituée d'un ensemble de pré-supposés sociaux et politique et inscrite dans l'objet, ce que Madeleine Akrich nomme les « scripts ».

Pour finir, aborder le cas de l'IMSI catcher jusque là peu exploré dans le milieu académique à travers la reconstitution permet de comprendre comment il fonctionne et d'expérimenter avec celui-ci ; de le situer ainsi dans le champ de la surveillance malgré le flou qui entoure ses usages ; et d'émettre des hypothèses quant à la pertinence d'appliquer cette méthodologie à d'autres objets de la surveillance ou d'autres objets techniques confidentiels.

Malgré toutes les difficultés liées à la nature même de l'objet et aux écueils méthodologiques, cela valait la peine d'aborder cet objet complexe qu'est l'IMSI catcher, comme nous allons le voir dans les dimensions développées dans 8.2 qui aborde le rapport du dispositif au code logiciel et à l'espace, et dans 8.3 qui présente les contres-mesures possibles et qui s'efforce de préciser le rôle du designer dans un tel projet de recherche.

8.2 Code, espace et opacité

Nous l'avons vu au cours de cette thèse, l'IMSI catcher est un objet de la surveillance, qu'il soit utilisé à des fins de recueil de données (interception de l'IMSI, interception de communications), d'influence voire de contrôle (envoi massif de messages afin de disperser des manifestations) ou encore d'espionnage (in-

dustriel notamment). Pour pouvoir exécuter les actions susmentionnées sur des données numériques dans une zone géographique délimitée, son mode opératoire repose d'une part sur l'exécution de code logiciel et d'autre part sur sa puissance d'émission qui définit un périmètre d'action et introduit donc une certaine spatialité. Toutefois, son rapport au code logiciel à la manière dont ses usages ont une influence sur l'espace et les mobilités n'est pas tout à fait à rapprocher de la notion de *code/space*[80] forgée par Dodge et Kitchin, en ce sens que l'IMSI catcher ne participe pas à la création d'un code/space au sens des deux géographes ; mais il relève plutôt d'un régime flexible et mobile de la surveillance.

Pour en comprendre les nuances, reprenons l'exemple donné par ceux-ci — la zone d'enregistrement de l'aéroport : celle-ci est d'abord délimitée visuellement par une série de barrières, de marquage, d'éléments de signalétique et de dispositifs de contrôle avec lesquels le voyageur doit interagir (pour scanner un QR code par exemple) ; effectivement, si le code logiciel qui permet de traiter automatiquement les données cesse de fonctionner (à l'occasion d'un bug ou d'une panne), alors la zone d'enregistrement se transforme en salle d'attente potentiellement chaotique. Or, l'IMSI catcher ne délimite pas une zone qui s'impose visuellement, et l'action de contrôle ne repose pas sur une action tangible (scanner un QR code par exemple). En effet, celui-ci intervient dans un espace hertzien imperceptible pour les usagers du réseau et qui dépend directement de sa puissance d'émission ; en outre, l'action de contrôle repose sur l'exploitation des ondes hertziennes, de fait celle-ci est aussi imperceptible pour les usagers. De plus, si l'IMSI catcher cesse de fonctionner pour quelconque raison, cela n'a aucun effet ni sur l'activité conduite dans la cellule (la zone délimitée par l'antenne relais), ni dans l'espace défini par cette même cellule, ni sur les usagers de la cellule. De la même manière, l'IMSI catcher ne produit pas tout à fait une « *software sorted geography* » telle que proposée par Stephen Graham (2005), en tout cas pas sur le fait (c'est-à-dire moment même de son utilisation). En effet, l'utilisation de l'IMSI catcher n'opère pas une discrimination qui empêche l'accès à tel ou tel lieu ; par contre, il donne lieu à la probabilité que l'on nous reproche d'avoir été à un endroit à un moment (manifestation, participation au crime organisé). Cela pose la question de la persistance des données collectées dans le temps et de la fiabilité de ces données en regard du mode opératoire « coup de filet » propre à l'IMSI catcher (qui collecte sans filtre toutes les données des téléphones à sa portée).

Toutefois, les conclusions tirées ici se heurtent à une limite de taille : l'IMSI catcher a été étudié en tant qu'objet technique indépendant et autonome. Afin de tirer des enseignements plus larges qui pourraient s'inscrire dans les études

80 Les deux géographes en donne la définition suivante : « un espace qui est dépendant du logiciel pour qu'il soit transduit comme prévu. Ici, la relation entre le logiciel et l'espace est dyadique ; ils sont constitués mutuellement, c'est-à-dire produits l'un à travers l'autre » (Dodge, Kitchin, 2011, p. 261).

surveillancielles il serait nécessaire d'étudier en détail le (ou les) système(s) socio-technique(s) dans le(s)quel(s) il s'insère ; c'est-à-dire le considérer dans l'écosystème complet (par exemple policier et judiciaire dans le cas de lutte anti-criminelle) dans lequel et pour lequel il est utilisé. En d'autres termes, cela revient à poser la question de l'usage des données après leur collecte : par qui sont-elles utilisées ? Sont-elles stockées ? Font-elles l'objet d'un traitement automatisé ? Malheureusement, ces questions dépassent largement le cadre d'étude de la thèse et demanderaient à être étudiées à travers d'autres projets de recherche.

Par ailleurs, une des hypothèses formulées au début de la thèse était que l'IMSI catcher dépassait le modèle du panoptique défini par Foucault (1975). Nous avons pu confirmer cette hypothèse ; en effet, l'IMSI catcher n'a pas besoin de la structure architecturale rigide du panoptique pour exercer son action (les espaces institutionnels cités par Foucault, tels que la prison, l'école ou encore l'hôpital). Au contraire plutôt qu'à un modèle solide et fixe, il s'apparenterait à un modèle flexible et mobile ; puisque le mode d'action de cet objet de la surveillance se rapprocherait de la notion avancée par Deleuze sur les sociétés de contrôle (1990) : en substance, il n'y a plus besoin d'un espace clos où exercer la surveillance puisque nous transitons constamment d'espace clos en espace clos (dans le cas présent les cellules téléphoniques) et nous portons sur nous une partie de l'infrastructure qui permet la surveillance (ce que Deleuze désigne comme un « collier électronique », dans le cas présent : le téléphone). Cette flexibilité et cette mobilité ne sont pas sans rappeler le modèle de surveillance liquide proposé par Baumann et Lyon en constante mouvance.

C'est aussi ici que réside l'intérêt de la démarche par le design, puisqu'elle amène une perspective du « faire » et elle permet d'expérimenter directement avec les aspects flexible, mobile et « liquide » de l'objet. En effet, il n'aurait pas été possible de faire l'expérience directe de ces aspects sur la base d'une analyse documentaire ; que ce soit dans l'aspect « liquide » en interceptant des données du réseau en constante activité, dans l'aspect mobile en allant écouter telle ou telle antenne relais dans le milieu urbain ou encore dans l'aspect flexible en mettant en place des réseaux cellulaires locaux afin de passer des appels entre différents participants d'un workshop. La démarche de recherche par le design permet ainsi de lever une partie de l'opacité qui recouvre l'IMSI catcher et amène une certaine transparence dans la connaissance de son fonctionnement. C'est ce qui est fait dans la performance 900 MHz : elle dévoile au public une partie de l'opacité du fonctionnement du réseau téléphonique mobile et par extension de l'IMSI catcher et rend compte de l'espace urbain « habité » par les ondes électromagnétiques. En outre, les prototypes produits lors du workshop *900 MHz: Protest* ainsi que le *BlocBalloon* sont un premier pas vers l'illustration et l'incarnation de cette surveillance liquide : en s'attaquant ou en contrant la surveillance rendue

possible par l'IMSI catcher ils permettent d'une part de la figurer et d'autre part de la dénoncer. De plus, ils sont des prototypes de modes d'emploi (ou des notes d'intention pour certains) pour des actions de contre-mesures à mettre en place pour aller vers une contre-surveillance, nécessaire pour s'interroger sur la légitimité de la surveillance, et ce à la fois dans les champs académiques mais aussi pour les organisations de défense des libertés.

8.3 Contre-surveillance et contre-mesures

La série d'objets de contestation produits au cours de la thèse met en lumière la contre-surveillance face à la surveillance liquide. Les pratiques de prévention, de défense ou de protection face à l'IMSI catcher sont ainsi différentes des contre-mesures que l'on peut adopter face à une caméra de surveillance par exemple. En effet, la plupart du temps la caméra de surveillance s'impose visuellement, elle est souvent fixe dans un milieu connu, et il est relativement facile de la contourner ou de se dissimuler avec des moyens analogiques (derrière un maquillage par exemple), même dans le cas où un traitement automatique des images est opéré (*CV Dazzle*, Harvey, 2010). Néanmoins, dans le cas de la surveillance liquide, il est de plus en plus difficile d'identifier les appareils de surveillance (drones, algorithmes sur les réseaux sociaux), notamment en raison de leur caractère flexible et mobile (traits que l'on retrouve dans le drone par exemple) ou de leur caractère imperceptible ou intangible (algorithmes sur les réseaux sociaux) qui repose souvent sur la méconnaissance d'un objet par son utilisateur — ce qui renvoie à la définition de la boîte noire au sens des STS de Vinck comme un objet dont on ignore ou dont on a oublié le fonctionnement interne.

Ainsi, il est nécessaire pour quiconque tente de le déjouer de connaître en détail le « champ de vision » de l'observateur ; c'est ce qu'a permis la phase de reconstitution : comprendre le fonctionnement de l'IMSI catcher et identifier ses failles et ses limites afin de « le battre sur son propre terrain ». C'est sur cette compréhension fine du principe de l'IMSI catcher qu'il a été possible de concevoir une série d'objets « antagonistes » reposant sur des principes de camouflage, de masquage, de brouillage ou encore d'obfuscation. Par exemple, comprendre le fait que l'IMSI catcher « attrape » les téléphones en émettant plus fort que les antennes relais et qu'un téléphone ne peut pas être associé à plus d'une antenne à la fois a servi à concevoir le *BlocBalloon* comme un IMSI catcher lui-même, puis de la même façon cela a permis d'imaginer l'obfuscation possible envers les dispositifs aux mains des forces de l'ordre en permettant l'émission d'IMSIs « leurres ». Si ces manières de déjouer la surveillance illustrent une forme de confrontation et de défiance face aux autorités, ces objets ne relèvent pas tout à fait du *adversarial design* (DiSalvo, 2012) : bien que comportant des éléments d'*agonisme* et de défiance, ceux-ci s'apparentent à des preuves de concept (ou

de faisabilité) plutôt qu'à des objets fonctionnels. Cette notion d'agonisme est nécessaire à la transformation de ces objets spéculatifs en des « objets adversariaux », ainsi comme le souligne la sociologue Chantal Mouffe :

> « Mobilization requires politicization, but politicizing cannot exist without the production of a conflictual representation of the world, with opposed claims, with which people can identify, thereby allowing for passions to be mobilized within the spectrum of the democratic process. » (Mouffe, 2005, p.25)

En d'autres termes, si on applique la citation au cas du *BlocBalloon* et des posters qui l'accompagnent, ceux-ci portent en eux cette représentation conflictuelle et ce potentiel affrontement avec les forces de l'ordre (de par sa forme de gonflable et son action sur le réseau téléphonique), mais pour réaliser pleinement ce processus politique et démocratique que décrit la sociologue, il serait nécessaire que les prototypes produits au cours cette thèse fassent leurs preuves sur le terrain en étant sortis du cadre de l'école ou de l'exposition, puis développés et testés par des hackers et des activistes par exemple. Dans l'état actuel, ils permettent déjà d'établir la discussion et de susciter des réactions auprès du grand public grâce au format de l'exposition par exemple (« *design for debate* », Dunne, 2008 ; « *discursive design* », Tharp et Tharp, 2018), mais aussi dans le champ académique de la recherche en design par les publications et la thèse. Malheureusement le vernissage du *BlocBalloon* à la Maison des Arts Électroniques à Bâle a eu lieu en ligne en raison des restrictions sanitaires COVID-19 : ce moment habituellement propice à la discussion et à la construction d'un débat s'en est trouvé largement affecté.

En outre, le démontage et la reconstitution de la boîte noire a permis la conception et la production d'une performance audiovisuelle à l'attention du grand public. Malgré tous les efforts consentis dans la mise en lumière de cette surveillance, l'IMSI catcher reste un objet technique complexe pour public profane et difficile à présenter sous une forme particulière. Rendre effectivement compte de l'emprise du dispositif sur le réseau téléphonique mobile est un exercice extrêmement délicat, toutefois le designer peut ici faire des choix esthétiques (qu'ils soient visuel ou sonores) afin de souligner certains aspects de cette surveillance, par exemple sa place, sa mobilité et sa fluidité dans l'espace urbain.

Aussi, là où les *surveillance studies* échouent à donner une échappatoire aux univers dystopiques dont elles rendent compte, le designer lui peut concevoir et donner à voir des alternatives à ceux-ci en proposant des objets qui contournent, détournent, contre-font la surveillance et qui ont une réelle portée politique et démocratique. Il y a ici une plus grande liberté et un avantage dans la posture du designer à établir une narration avec des moyens qui lui sont propres et à participer à la production de connaissance ; sans que cette liberté ne vienne entacher la rigueur épistémologique du projet de recherche. En effet, si une

partie de la pratique du design repose sur des intuitions ou des pré-supposés, la méthodologie déployée dans cette thèse repose sur une documentation précise et une vérification de toute assertion qui permettent une rigueur scientifique et de produire des connaissances, et ce malgré le recours à des méthodes expérimentales et une conception et production formelle de différents artefacts

C'est aussi ce que les scénarios produits dans le chapitre 7 « Recherche par le design III : Vers le *design fiction* » tentent d'explorer de manière prospective : les futurs possibles et probables de cette surveillance en lien avec les différents acteurs sur le terrain. En effet, les scénarios proposent trois futurs potentiels de l'IMSI catcher dans un paysage de la surveillance qui convoque les citoyens, les chercheurs, les forces de l'ordre et les activistes.

De la même manière, le designer peut se défaire d'une certaine contrainte de temporalité : l'immédiateté du faire et du prototypage permet au designer de se défaire de la contrainte de évolution si chère à Simondon, et à ne pas prendre un objet dans une temporalité longue au contraire de l'histoire des techniques, qui considère l'objet dans de longues « lignées ». Cela permet dans le cas particulier de l'IMSI catcher de contourner son caractère confidentiel et sa rareté, et de travailler dans une certaine urgence pour s'emparer un sujet politique en cours, qui n'est pas encore cristallisé dans l'histoire. Cette position singulière du designer permet là encore une production épistémologique si elle est faite avec une méthodologie rigoureuse.

Le rôle du designer résiderait ainsi dans la monstration non seulement de phénomènes techno-politiques mais aussi et surtout dans la présentation d'autres trajectoires possibles que celles pressenties dans les *surveillance studies*. En effet, les trajectoires abordées dans les scénarios du chapitre 7 montrent différentes alternatives socio-politiques plus ou moins plausibles : d'un avènement presque utopique de la 2G comme domaine public mais qui fait émerger la constitution de milices et de nouvelles formes de conflit ; à un totalitarisme sécuritaire étatique dystopique qui fait émerger de nouvelles formes de résistances. Néanmoins, on se trouve parfois limité par le paradoxe de la vie privée : si l'on met en lumière des phénomènes qui mettent en danger certaines libertés individuelles, il est quasi-impossible de quantifier l'impact que cela a réellement sur les habitudes des individus et on peut facilement imaginer que ceux-ci ne changent pas drastiquement leur relation aux technologies numériques pour autant.

Ainsi, comme nous avons pu le voir, il est pertinent de traiter un objet aussi complexe que l'IMSI catcher sous ses différentes facettes par une démarche de recherche en design ; et cela soulève une opportunité liée à l'application de la méthodologie déployée dans la thèse pour traiter d'autres objets de la surveillance — les algorithmes de reconnaissance de la démarche utilisés dans la vidéosurveillance par exemple ou bien encore l'utilisation du RFID à des fins de

tracking (proche de la démarche d'Arnall) — éventuellement adaptée afin qu'elle puisse être destinée aux acteurs suivant : les activistes, les organismes publiques, les associations, les chercheurs en *surveillance studies* et enfin les chercheurs en design. Il serait possible de déployer une méthodologie basée sur (1) un processus de reconstitution, (2) la production de contenu « médiationnel » rendant compte de cette reconstitution, sous forme de performance audiovisuelle ou de documentaire, (3) la conception d'objets désobéissants qui questionnent l'objet abordé et (4) l'élaboration de scénarios prospectif (ou de design fictions) donnant des alternatives au présent de l'objet en question. Cette méthodologie pourrait notamment intéresser les organisations de défense des libertés citées en introduction que sont EFF, Privacy International ou la Quadrature du Net, et être utilisée dans le cadre d'ateliers participatifs concernant un public plus large que celui auquel s'adresse cette thèse.

Néanmoins, au cours de cette thèse, je me suis principalement attaché à l'étude de l'IMSI catcher dans un contexte particulier, celui où on le trouve le plus fréquemment : la manifestation, où il serait le plus souvent utilisé pour relever l'identité des téléphones en présence, et dans certains cas pour l'envoi de messages en masse à des fins de dissuasion et de dispersion. Ainsi une limite évidente apparait, puisque l'IMSI catcher est aussi utilisé dans des contextes d'espionnage étatique, d'espionnage industriel, de surveillance d'individus dans des affaires criminelles, de contrôle aux frontières qui constituent autant de champs à couvrir. Même s'ils ont été en partie abordés dans les scénarios de design fiction, c'est un prolongement possible du travail de cette thèse. Il en est de même pour la question de la disparition de la 2G[81] et de l'apparition de la 5G que je n'ai fait que brièvement évoquer. Dans les pays occidentaux, il est fort probable que l'arrivée des protocoles 5G, annoncés comme plus sécurisés, soit accompagnée de son lot de nouveaux outils de surveillance et mérite ainsi une attention toute particulière des chercheurs en *surveillance studies* d'une part, et des chercheurs en design d'autre part.

Enfin, devant l'apparente complexité et dangerosité d'un dispositif de surveillance qui au final « ne fait que » intercepter un identifiant ou quelques communications GSM, on serait en mesure de se demander si le recours à celui-ci relève d'un phénomène global et massif et si les nombreuses craintes évoquées dans cette thèse sont justifiées. Un élément de réponse à cette question réside dans la récente décision de Google d'intégrer à Android la possibilité de désactiver la 2G sur son téléphone[82] (donc de l'empêcher de « tomber » sur la 2G si les protocoles plus récents et plus sécurisés 3/4/5G ne sont pas disponibles) et qui tend à montrer qu'il y a tout de même encore des risques à craindre.

81 Ce qui est largement avancé dans les pays occidentaux mais pas nécessairement dans le reste du monde, où encore beaucoup de services reposent sur la 2G.

82 <https://www.bleepingcomputer.com/news/security/android-users-can-now-disable-2g-to-block-stingray-attacks/> consulté le 15.02.2022.

Bibliographie

Abrams, Janet, et Peter Hall, éd. *Else/Where New Cartographies of Networks and Territories*. Minneapolis, Minn: Univ. of Minnesota Design Institute, 2005.

Aim, Olivier. *Les théories de la surveillance: Du panoptique aux Surveillance Studies.* Armand Colin, 2020.

Akrich, Madeleine. « Comment décrire les objets techniques ? » *Techniques & Culture. Revue semestrielle d'anthropologie des techniques*, no 9 (1 septembre 1987). https://doi.org/10.4000/tc.863.

———. « The De-scription of Technical Objects ». In *Shaping Technology/Building Society. Studies in Sociotechnical Change*, 205. MIT Press, 1992. https://halshs.archives-ouvertes.fr/halshs-00081744.

Allard, Laurence. « L'engagement du chercheur à l'heure de la fabrication numérique personnelle ». Hermes, *La Revue n° 73*, no 3 (11 décembre 2015): 159-67.

Arnall, Timo. « Making Visible », 2014. https://aho.brage.unit.no/aho-xmlui/handle/11250/2364779.

Auger, James. « Speculative Design: Crafting the Speculation ». *Digital Creativity 24*, no 1 (1 mars 2013): 11-35. https://doi.org/10.1080/14626268.2013.767276.

Ball, Kirstie, Kevin Haggerty, et David Lyon, éd. *Routledge Handbook of Surveillance Studies*. Paperback ed. Routledge International Handbooks. London: Routledge, 2012.

Barnes, Susan B. « A Privacy Paradox: Social Networking in the United States ». *First Monday*, 4 septembre 2006. https://doi.org/10.5210/fm.v11i9.1394.

Bauman, Zygmunt. *Liquid Modernity*. Cambridge, UK : Malden, MA: Polity Press ; Blackwell, 1999.

Bauman, Zygmunt, et David Lyon. *Liquid Surveillance: A Conversation*. Polity conversations series. Cambridge, UK ; Malden, MA: Polity Press, 2012.

Bentham, Jeremy. *The Panopticon Writings*, 1787.

Berger, Gaston, Jacques de Bourbon Busset, et Pierre Massé. *De la prospective: textes fondamentaux de la prospective française; 1955-1966*. Édité par Philippe Durance. Prospective. Paris: L'Harmattan, 2007.

Bleecker, Julian. « Design Fiction: A Short Essay on Design, Science, Fact and Fiction ». Near Future Laboratory, 2009.

Blythe, Mark. « Research through design fiction: Narrative in real and imaginary abstracts ». *Conference on Human Factors in Computing Systems - Proceedings*, 26 avril 2014. https://doi.org/10.1145/2556288.2557098.

Brown, Barry, Julian Bleecker, Marco D'Adamo, Pedro Ferreira, Joakim Formo, Mareike Glöss, Maria Holm, et al. « The IKEA Catalogue: Design Fiction in Academic and Industrial Collaborations ». *In Proceedings of the 19th International Conference on Supporting Group Work*, 335-44. GROUP '16. New York, NY, USA: Association for Computing Machinery, 2016. https://doi.org/10.1145/2957276.2957298.

Brunton, Finn, et Helen Nissenbaum. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA, USA: MIT Press, 2015.

Cardon, Dominique. « Le design de la visibilité ». *Reseaux* n° 152, no 6 (2008): 93-137.

Castagnino, Florent. « Critique des surveillances studies. Éléments pour une sociologie de la surveillance ». *Deviance et Societe* Vol. 42, no 1 (29 mars 2018): 9-40.

Coulton, Paul, Dan Burnett, et Adrian Gradinar. « Games as Speculative Design: Allowing Players to Consider Alternate Presents and Plausible Features », 2016. https://doi.org/10.21606/drs.2016.15.

Coulton, Paul, Joseph Lindley, Miriam Sturdee, et Mike Stead. « Design Fiction as World Building », 2017. https://doi.org/10.6084/m9.figshare.4746964.

Cross, Nigel. « Designerly Ways of Knowing ». *Design Studies*, Special Issue Design Education, 3, no 4 (1 octobre 1982): 221-27. https://doi.org/10.1016/0142-694X(82)90040-0.

Dautrey, Jehanne, et Emanuele Quinz, éd. *Strange design: du design des objets au design des comportements*. Villeurbanne: It : Éditions, 2014.

Deforge Yves. *Technologie et génétique de l'objet industriel*. Collection Université de Compiègne. Paris: Maloine, 1985.

Delaunay, Quynh. *Histoire de la machine à laver: un objet technique dans la société française*. Histoire. Rennes: Presses universitaires de Rennes, 1994.

Deleuze, Gilles. *Foucault*. Paris: Éditions de Minuit, 1986.

———. « Post-scriptum sur les sociétés de contrôle ». *Pourparlers* 1972-1990, 1990.

Dessauce, Marc et Architectural League of New York. *The Inflatable Moment: Pneumatics and Protest in '68*. New York: Princeton Architectural Press, 1999.

DiSalvo, Carl. *Adversarial Design*. Design Thinking, Design Theory. Cambridge, MA, USA: MIT Press, 2012.

Dunne, Anthony. « Design for Debate ». *Architectural Design* 78 (1 novembre

2008): 90-93. https://doi.org/10.1002/ad.779.

———. *Hertzian Tales: Electronic Products, Aesthetic Experience, and Critical Design*. Cambridge, MA, USA: MIT Press, 1999.

Dunne, Anthony, et Fiona Raby. *Speculative Everything: Design, Fiction, and Social Dreaming*. Cambridge, MA, USA: MIT Press, 2013.

Eggen, Per-Odd, Lise Kvittingen, Annette Lykknes, et Roland Wittje. « Reconstructing Iconic Experiments in Electrochemistry: Experiences from a History of Science Course ». *Science & Education* 21 (1 février 2012): 179-89. https://doi.org/10.1007/s11191-010-9316-1.

Fallan, Kjetil. *Design History: Understanding Theory and Method.* New York: Berg Publishers, 2010.

Farman, Jason. « Surveillance from the Middle: On Interception, Infrastructure, and the Material Flows of Asynchronous Communication ». *Media Fields* 11 (1 janvier 2016).

Findeli, Alain. « Searching For Design Research Questions: Some Conceptual Clarifications ». In *Questions, Hypotheses & Conjectures*, par Rosan Chow, Gesche Joost, et Wolfgang Jonas, 278-93, iUniverse éd. Berlin, 2010.

Findeli, Alain, et Rabah Bousbaci. « L'Eclipse de L'Objet dans les Théories du Projet en Design (The Eclipse of the Object in Design Project Theories) ». *The Design Journal* 8 (1 novembre 2005): 35-49. https://doi.org/10.2752/146069205789331574.

Findeli, Alain, et Anne Coste. « De la recherche-création à la recherche-projet : un cadre théorique et méthodologique pour la recherche architecturale ». *Lieux-communs* 10 (1 janvier 2007).

Flood, Catherine, et Gavin Grindon. *Disobedient Objects*. Harry N. Abrams, 2014.

Foucault, Michel. *Surveiller et punir: naissance de la prison*, 1975.

Fourmentraux, Jean-Paul. *AntiDATA: la désobéissance numérique: art et hacktivisme technocritique*. Collection « Perceptions ». Dijon: Les Presses du réel, 2020.

Frayling, Christopher. « Research in Art and Design ». *Research in Art and Design (Royal College of Art Research Papers, Vol 1, No 1, 1993/4)*, 1994. https://researchonline.rca.ac.uk/384/.

Gauthier, Philippe. « Création contre science en design, les conditions d'un vrai débat : réponse à Lysianne Léchot Hirt ». Sciences du Design n° 2, no 2 (2015): 65-70.

Goguey, Félicien. « Catch Me If You Can: Designing a Disobedient Object to Protest Against GSM Surveillance ». In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-7. New York, NY, USA: Association for Computing Machinery, 2021. https://doi.org/10.1145/3411763.3450363.

———. « Remaking an IMSI Catcher ». *Continent*. Issue 8.1-2 (2019): 176-85.

Graham, Stephen. *Cities Under Siege: The New Military Urbanism.* Verso Books, 2010.

———. « Software Sorted Geographies ». *Progress in Human Geography* 29 (1 octobre 2005). https://doi.org/10.1191/0309132505ph568oa.

Herrz, Garnet. *Critical Making*, 2012.

Hertz, Garnet. *Disobedient Electronics: Protest*, 2018.

Huhtamo, Erkki. *Illusions in Motion: Media Archaeology of the Moving Panorama and Related Spectacles*. Leonardo. Cambridge, MA, USA: MIT Press, 2013.

Huxley, Aldous. *Le Meilleur des mondes*. 1932e éd. Paris: Plon, 1931.

Hwang, Tim. *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*. First edition. FSG Originals x Logic. New York: FSG Originals, Farrar, Straus and Giroux, 2020.

Kitchin, Rob, et Martin Dodge. *Code/Space: Software and Everyday Life*. MIT Press, 2014.

Kittler, Friedrich A. *Gramophone, film, typewriter*. Médias / théories. Dijon: les Presses du réel, 2018.

Koskinen, Ilpo, John Zimmerman, Thomas Binder, Johan Redström, et Stephan Wensveen. *Design Research Through Practice: From the Lab, Field, and Showroom. Professional Communication, IEEE Transactions on*. Vol. 56, 2011. https://doi.org/10.1109/TPC.2013.2274109.

Krippendorff, Klaus. *The Semantic Turn A New Foundation for Design*. Boca Raton: CRC/Taylor & Francis, 2006.

Latour, Bruno. *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, Mass: Harvard University Press, 1999.

Léchot Hirt, Lysianne, éd. *Recherche-création en design: modèles pour une pratique expérimentale*. Genève: Mētis Presses, 2010.

Léchot-Hirt, Lysianne. « Recherche-création en design à plein régime : un constat, un manifeste, un programme ». *Sciences du Design* n° 1, no 1 (27 mai

2015): 37-44.

Leroi-Gourhan, André. *Milieu et Techniques*. Reprod. et impr. [D. Ausg. 1973]. Sciences d'aujourd'hui 2. Paris: Ed. Albin Michel, 1945.

LOI n° 2015-912 du 24 juillet 2015 relative au renseignement (1), 2015-912 § (2015).

Lyon, David. *Surveillance Studies: An Overview*. Polity, 2007.

———. T*he Electronic Eye: The Rise of Surveillance Society.* University of Minnesota Press, 1994. https://www.jstor.org/stable/10.5749/j.ctttsqw8.

Mackenzie, Adrian. *Wirelessness: Radical Empiricism in Network Cultures.* Cambridge, MA, USA: MIT Press, 2010.

Malpass, Matt. *Critical Design in Context: History, Theory, and Practice*. London ; New York: Bloomsbury Academic, an imprint of Bloomsbury Publishing Plc, 2017.

Marx, Gary. « A Tack in the Shoe: Neutralizing and Resisting the New Surveillance ». *Journal of Social Issues - J SOC ISSUES* 59 (1 juin 2003): 369-90. https://doi.org/10.1111/1540-4560.00069.

Marx, Gary T. « Surveillance Studies ». In *International Encyclopedia of the Social & Behavioral Sciences*, 733-41. Elsevier, 2015. https://doi.org/10.1016/B978-0-08-097086-8.64025-4.

———. *Undercover: Police Surveillance in America.* University of California Press, 1988. https://www.jstor.org/stable/10.1525/j.ctt1ppg2c.

Marx, Gary T., et Sanford Sherizen. « Monitoring On The Job: How to Protect Privacy as Well as Property ». *Technology Review*, décembre 1986. https://web.mit.edu/gtmarx/www/privacy.html.

Mattelart, Armand. *La globalisation de la surveillance: Aux origines de l'ordre sécuritaire*. La Découverte, 2008.

Michel, Ralf. *Design Research Now: Essays and Selected Projects*. Basel: Birkhäuser, 2007.

Midal, Alexandra. *Design, l'anthologie: 1841-2007*. Saint-Étienne, Genève: Cité du design-École supérieure d'art et de design, HEAD – Genève, 2013.

Mouffe, Chantal. *On the political. Thinking in action*. London ; New York: Routledge, 2005.

Near Future Laboratory. *The Manual of Design Fiction*, 2021. https://nearfuturelaboratory.myshopify.com/products/the-manual-of-design-fiction.

Ney, Peter, Ian Smith, Gabriel Cadamuro, et Tadayoshi Kohno. « SeaGlass: Enabling City-Wide IMSI-Catcher Detection ». *Proceedings on Privacy Enhancing Technologies* 2017 (1 juillet 2017). https://doi.org/10.1515/popets-2017-0027.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford University Press, 2009.

Nova, Nicolas. « Figures mobiles: une anthropologie du smartphone ». University of Geneva, 2018. https://doi.org/10.13097/archive-ouverte/unige:107645.

———. *Futurs ? la panne des imaginaires technologiques.* Bibliothèque des miroirs. Montélimar: les Moutons électriques, 2014.

Nova, Nicolas, et Anaïs Bloch. *Dr. Smartphone: An Ethnography of Mobile Phone Repair Shops*, 2020.

Nova, Nicolas, et Laurent Bolli. *Joypads ! le design des manettes*. Bibliothèque des miroirs. Lyon: les Moutons électriques éd, 2013.

Nova, Nicolas, et Félicien Goguey. « Le black fax et ses dérivés ». *Techniques Culture* n° 74, no 2 (10 décembre 2020): 150-51.

Oliveira, Pedro, et Luiza Prado. « Designer/Shapeshifter: A De-Colonial Redirection for Speculative and Critical Design ». In *Tricky Design: The Ethics of Things*, édité par Tom Fisher et Lorraine Gamman, 2018. https://ebookcentral.proquest.com/lib/umontreal-ebooks/detail.action?docID=5568260.

Oliver, Julian, Gordan Savičić, et Danja Vasiliev. « The Critical Engineering Manifesto », 2011. https://criticalengineering.org/fr.

Orwell, George. 1984. Paris: Gallimard, 1949.

Papanek, Victor. *Design pour un monde réel*, 1971.

Parikka, Jussi. *What is Media Archaeology?* Cambridge, UK ; Malden, MA: Polity Press, 2012.

Parikka, Jussi, et Quentin Julien-Saavedra. « Archéologie des media et arts médiaux ». *Multitudes* n° 59, no 2 (11 juin 2015): 206-16.

Parks, Lisa. « Rise of the IMSI Catcher ». *Media Fields* 11 (1 janvier 2016).

———. « Technostruggles and the Satellite Dish: A Populist Approach to Infrastructure ». In *Cultural Technologies*. Routledge, 2012.

Poitras, Laura. *Astro Noise: A Survival Guide for Living Under Total Surveillance.* New York: Whitney Museum of American Art, 2016.

Quinz, Emanuele. *Le cercle invisible: environnements, systèmes, dispositifs.*

Figures. Dijon: les Presses du réel, 2017.

Ratto, Matt, et Megan Boler, éd. *DIY Citizenship: Critical Making and Social Media*. Cambridge, MA, USA: MIT Press, 2014.

Rijsbergen, K. « The Effectiveness of a Homemade IMSI Catcher Build with YateBTS and a BladeRF ». *Undefined*, 2016. https://www.semanticscholar.org/paper/The-effectiveness-of-a-homemade-IMSI-catcher-build-Rijsbergen/e09781188bcafafbecbffe1a380a7708fad0d438.

Rittel, Horst W. J., et Melvin M. Webber. « Dilemmas in a General Theory of Planning ». *Policy Sciences* 4, no 2 (1 juin 1973): 155-69. https://doi.org/10.1007/BF01405730.

Rose, Gillian. *Visual Methodologies: An Introduction to Researching with Visual Materials*. 4th edition. London: SAGE Publications Ltd, 2016.

RS 312.0 - Code de procédure pénale suisse du 5 octobre 2007 (Code de procédure pénale, CPP) (2007). https://www.fedlex.admin.ch/eli/cc/2010/267/fr.

Rule, James B. *Private Lives and Public Surveillance: Social Control in the Computer Age.* New York: Schocken Books, 1973.

Sayers, Jentery. « Prototyping the Past ». Visible Language 49.3, 2015. https://www.semanticscholar.org/paper/Prototyping-the-Past-Sayers/5794c013d87b731d261c057c3a0ad57bcb130f90.

———. « The Relevance of Remaking », 2014. https://maker.uvic.ca/remaking/.

Scheidt, Konstanze. « Inflatables and Activism ». *A Peer-Reviewed Journal About* 7 (6 juillet 2018): 128-38. https://doi.org/10.7146/aprja.v7i1.116060.

Schwartz, Peter. *The Art of the Long View: Planning for the Future in an Uncertain World*. Currency Paperback. New York: Currency Doubleday, 1991.

Simondon, Gilbert. *Du mode d'existence des objets techniques.* Paris: Aubier, 1958.

Sterling, Bruce. *Shaping Things*. Mediaworks Pamphlets. Cambridge, MA, USA: MIT Press, 2005.

Stiegler, Bernard, éd. *Digital studies: organologie des savoirs et technologies de la connaissance.* Collection du nouveau monde industriel. Limoges: Fyp éditions, 2014.

Strobel, Daehyun. « IMSI Catcher ». Ruhr-Universität Bochum, 2007.

Taylor, Frederick Winslow. *The Principles of Scientific Management*. Londres, New York: Harper & Brothers, 1911.

Tharp, Bruce M., et Stephanie M. Tharp. *Discursive Design: Critical, Speculative, and Alternative Things*. Design Thinking, Design Theory. Cambridge, MA, USA: MIT Press, 2019.

Thwaites, Thomas. *The Toaster Project: Or A Heroic Attempt to Build a Simple Electric Appliance from Scratch*. 1st ed. New York: Princeton Architectural Press, 2011.

Tonkinwise, Cameron. « How We Intend to Future: Review of Anthony Dunne and Fiona Raby, Speculative Everything: Design, Fiction, and Social Dreaming ». *Design Philosophy Papers* 12 (1 décembre 2014). https://doi.org/10.2752/144871314X14159818597676.

Vial, Stéphane. « Qu'est-ce que la recherche en design ? Introduction aux sciences du design ». *Sciences du Design* n° 1, no 1 (27 mai 2015): 22-36.

Vinck, Dominique. « De l'objet intermédiaire à l'objet-frontière. Vers la prise en compte du travail d'équipement ». *Revue d'anthropologie des connaissances* 3, 1, no 1 (2009): 51-72. https://doi.org/10.3917/rac.006.0051.

———. Sociologie des Sciences. Paris, Armand Colin, 1995. https://halshs.archives-ouvertes.fr/halshs-00273041.

Weber, Max. *Économie et société*, 1921.

Wiener, Norbert. *Cybernetics or Control and Communication in the Animal and the Machine*, 1948.

Ziewitz, Malte. « Governing Algorithms: Myth, Mess, and Methods ». *Science, Technology, & Human Values* 41, no 1 (1 janvier 2016): 3-16. https://doi.org/10.1177/0162243915608948.

Remerciements

Je tiens à remercier tout particulièrement mes directeurs de thèse, Frédéric Kaplan et Nicolas Nova pour avoir accepté de diriger ce travail, pour leur soutien indéfectible et bienveillant ainsi que pour leurs conseils avisés tout au long de ce parcours.

Mes remerciement vont aussi aux membres du jury Laurence Allard, Emanuele Quinz et Jérôme Baudry, qui ont accepté de participer à l'évaluation de ce travail et pour leurs suggestions et leurs remarques constructives, de même que Jérôme Chenal qui a accepté de prendre part à la présidence du jury.

Je remercie Anne-Catherine Sutermeister qui a initié le partenariat doctoral HEAD – EPFL et Anthony Masure qui en a pris la relève ainsi que Jean-Pierre Greff pour l'avoir rendu possible.

Je remercie de plus Salômé Guillemin, Alexia Mathieu, Marta Revuelta, Nicolas Baldran, Lysianne Léchot-Hirt, Alexandra Midal, Luca Pattaroni, Daniel Pinkas, Daniel Sciboz, Gordan Savičić, Selena Savic, Julian Oliver, Carmen Weisskopf, Domagoj Smoljo, les étudiant.e.x.s du Master Media Design, David-Olivier Lartigaud, Sylvain Métille, Boris Magrini, Sabine Himmelsbach, la Art Foundation Pax et mes parents pour leur soutien et leur contribution.

À Lysianne, qui un soir d'avril 2016 m'a lancé : « Et la thèse, t'y penses ? »

Mis en page par Félicien Goguey et Salômé Guillemin.

Ce document a été rédigé en Markdown et mis en page avec le logiciel Indesign.
Le texte est composé en police Roboto Mono et PT Serif.

Mai 2022
<http://felicien.io>