UNIVERSITÉ DU QUÉBEC À MONTRÉAL

TrAVAIL PRATIQUE

IMSI-catcher

TRAVAIL PRÉSENTÉ à

Anne-sophie letellier

dans le cadre du cours

inm6000 Groupe 30

Guillaume Blouin

bLOG09079006

7 JUILLET 2021

# TABLE DES MATIÈRES

[TABLE DES MATIÈRES 2](#_Toc53574216)

[Introduction 3](#_Toc53574217)

[Acteurs principaux](#_Toc53574218) 5

[Fonctionnalités](#_Toc53574221) 6

[Vie privée](#_Toc53574222) 6

[Dommages collatéraux](#_Toc53574223) 7

[CONCLUSION](#_Toc53574224) 9

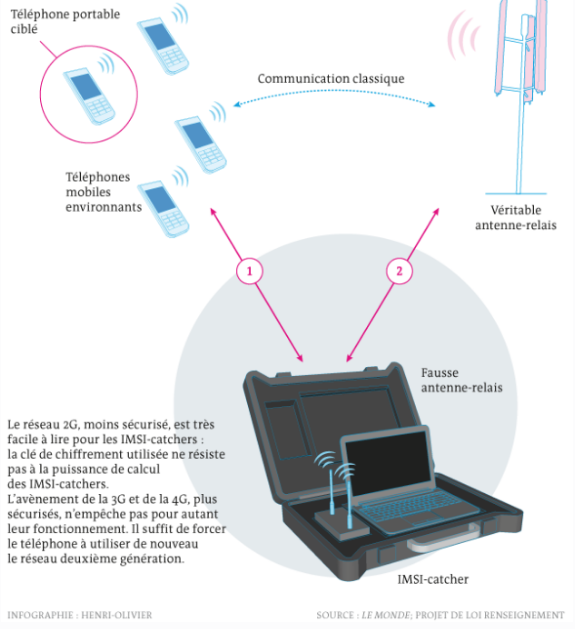
[BIBLIOGRAPHIE](#_Toc53574225) 10

# INTRODUCTION

De nos jours, les débats sur la surveillance électronique sont entendus depuis des lustres déjà. Quoi qu’il en soit, de nouvelles façons de faire de l’espionnage de masse ou ciblé sont toujours biens reçues par les autorités. En effet, alors que la surveillance électronique fait son appararition dans les années 80 selon le site officiel de la sécurité publique du Canada, sous forme de bracelets électroniques comme alternative à l’emprisonnement, cette technologie semble être appréciée par nos dirigeants et peut-être même par tout le monde. Par contre, nous en sommes maintenant à un moment opportuniste, après l’installation de systèmes de surveillance informatique ultra-secret par la NSA selon Radio-Canada et encore concernant l’espionnage des utilisateurs de téléphones mobiles, vous vous douterez que ces surveillances feront moins l’unanimité. La surveillance électronique servait autrefois à surveiller l’emplacement des probationnaires, délinquants réinsérés; celles plus modernes, comme les systèmes de surveillance téléphonique sont spécialement utiles pour enquêter, identifier à l’avance les projets illégaux mais désagréables, mal reçus par la population. Selon Martin Ouellet-Diotte, de «EXPLORA», les corps policiers du Canada utilisent la technologie «StingRay» depuis au moins les révélations d’Edward Snowden en 2013 (sous-traitant de la CIA devenu lanceur d’alerte).



En fait, le «StingRay», selon Wikipedia, ce serait : « Un IMSI-catcher, parfois traduit en intercepteur d'IMSI, est un appareil de [surveillance](https://fr.wikipedia.org/wiki/Surveillance) utilisé pour intercepter le trafic des [communications mobiles](https://fr.wikipedia.org/wiki/Téléphonie_mobile), récupérer des informations à distance ou pister les mouvements des utilisateurs des terminaux. Le terme *IMSI-catcher* est en réalité non exhaustif, l'appareil permettant de faire bien plus que simplement récupérer le numéro [IMSI](https://fr.wikipedia.org/wiki/International_Mobile_Subscriber_Identity). Pour arriver à ses fins, un IMSI-catcher simule une fausse [antenne-relais](https://fr.wikipedia.org/wiki/Antenne-relais_de_téléphonie_mobile) en s'intercalant entre le réseau de l'[opérateur de téléphonie](https://fr.wikipedia.org/wiki/Opérateur_de_téléphonie_mobile) et le matériel surveillé. » et ressemblerait à une valise facile à transporter muni d’un ordinateur et des antennes, ou alors une boite électronique qu’on peut connecter ou même encore des antennes et des périphériques adaptés séparés.

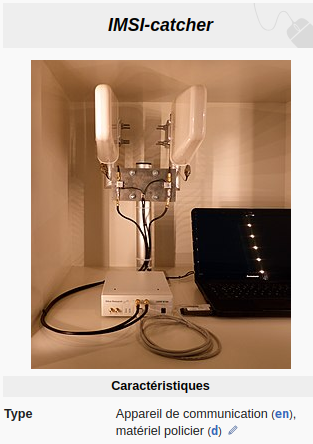


Ce serait intéressant d’en apprendre davantage sur cette fausse antenne pour déterminer si le feu en vaut la chandelle. L’usage de cet appareil peut alimenter les controverses et nous devront y voir plus clair; nous devrons déterminer qui sont les principaux usagers, quels sont leurs objectifs, et où se les procurent-ils, comment l’appareil collecte les données, y a-t-il des dommages collatéraux. En somme, ces aspects nous guideront pour bien comprendre le dilemme éthique et s’il y a lieu, quelles actions seraient recommandées.

# Acteurs principaux

Les sources diverses disent, les principaux usagers des systèmes de surveillance de téléphonie mobile sont les autorités sous toutes leurs formes, partout dans le monde. Selon [Martin Untersinger](https://www.lemonde.fr/signataires/martin-untersinger/) de «Le Monde», ce type d’appareil se marchande aux alentours de 100000 euros par «Cambridge Consultants», entreprise britannique, aussi par la société Gamma, disponible en ligne ou encore certains sites de ventes en ligne chinois. L'Europe a toutefois interdit la vente de ces appareils à la Syrie et à l’Iran. Le corps policier serait le grand champion de ce type d’espionnage, et même selon «EXPLORA», on nous dit: « ce type de technologie est fréquemment utilisé pour s’attaquer au crime organisé et pour débusquer des cellules terroristes». De tout évidence, cette technologie offerte aide beaucoup pour attraper les malfaiteurs. Radio-Canada ajoute par exemple: «La police de Vancouver a admis avoir utilisé le système de surveillance téléphonique contesté StingRay au moins une fois ».

Les gouvernements ne seraient pas les seuls à utiliser les équipements de surveillance de téléphonie. Effectivement, le privé spécialisé a aussi investi là dedans: « c’est un outil qui est utlisé sur le territoire français, en totale illégalité, par des structures qui ne dépendent pas de l’état. » a souligné le député de France, Jean-jacques Urvoas en juin 2013 dans « Le Monde ».



# F**onctionnalités**

Citons encore l’article parue dans « Le Monde » pour bien comprendre le mécanisme vulgarisé des ISMI-catchers: « Historiquement, les IMSI-catchers exploitent une faille de sécurité dans le réseau 2G : si le téléphone doit s’authentifier auprès de l’antenne-relais, « le téléphone, lui, n'authentifie pas le réseau auquel il se connecte », précise Philippe Langlois, fondateur et président de l’entreprise de sécurité P1 Security. Cette brèche a été corrigée dans les réseaux plus modernes (3G, 4G), mais les IMSI-catchers peuvent forcer le téléphone à se connecter en 2G et donc toujours exploiter cette faille. »; l’échange de sms, l’interception du trafic Internet mobile ou la gestion des appels entrants sont des fonctionnalités supplémentaires pouvant être disponibles sur ces outils d’espionnage. Le pire et le meilleur en même temps, c’est l’effet «ni vu ni connu» des espions car les ciblés ne savent pas qu’ils sont hackés. Selon Noa Ouziel, du site «firstpoint-mg.com», elle appelle ça: « This type of hack is also known as a man-in-the-middle (MitM) attack. »; attaque connue comme étant une interception des échanges entre deux personnes mais ici c’est un interception entre la personne et l’antenne relais, nul besoin d’un second interlocuteur. C’est selon les demandes de réseaux cellulaires du client de téléphonie mobile et nous pourrons connaître un peu de tout sur lui.

## **Vie privée**

Alors que nos réels moments privés s’amenuisent par la présence des appareils intelligents, collecteurs de données pour chaque instant d’utilisation, d’autres préoccupations dépassent largement la divulgation de renseignements personnels consciente, c’est-à-dire l’appropriation sournoise des ondes cellulaires sur la majorité des canadiens. C’est un sujet d’intérêt pour nous, ceux qui ont la vie privée à coeur peuvent avoir de nombreuses inquiétudes car ces dispositifs sont conçus pour écouter tout le monde et non pas juste des écoutes ciblés rappelle Martin Untersinger, de «Le Monde». Les appareils, dont nous apprenons l’existence, plus ou moins sophistiqués, sont capable d’intercepter les discussions des bandits mais au prix de balancer toutes les données de tous les usagers des antennes cellulaires au bras des autorités et autres inconnus sans mandat et respect pour les contribuables, citoyens. Le fait que des révélations soient faites aux moments où des fuites de données surviennent, et seulement à ces moments conjurons le, celles de Snowden en 2013 par exemple, « Je pourrais, en étant simplement assis à mon bureau, surveiller les échanges en ligne de n'importe qui, de vous, de votre comptable, d'un juge fédéral ou même du président si j'ai une adresse courriel personnelle. » montre une piètre transparence des autorités compétentes à ce sujet par rapport à la divulgation des outils qu’ils utilisent. Pour la surveillance de téléphonie mobile, autant que si c’est sur tout le monde l’écoute, faire des tests ou si c’est ciblé et réussit, ou bien pour arrêter quelqu’un qu’on aimerait bien savoir derrère les barreaux, ce serait grandement grâce à notre indulgence quant à laisser lui ou l’autre pouvoir nous écouter à la maison. L’idée que le moins de criminels en savent sur les technologies mises aux dispositions des agents de la paix, plus les résultats pertinents liés à l’usage de ces technologies seront élevés, est retenue par les défenseurs de l’ordre. Selon M. Untersinger, le FBI a dit: « trop en dire sur ces appareils risquerait de donner aux hors-la-loi les moyens de les détecter et de les contourner. Actuellement, une vingtaine d’Etats américains au moins utilisent des IMSI-catchers. », et défend le silence des autorités américaines.

## **Dommages collatéraux**

En général, monsieur et madame tout le monde continuent à utiliser leurs téléphones mobiles puisqu’ils en ont besoin au travail, pour la famille, etc. et l’intérêt des utilisateurs de la technologie de surveillance de téléphonie est de trouver des informations spéciales que les gens ordinaires, à toute première vue, n’ont sûrement pas alors nous pourrions admettre que ces appareils ont leur place parmis nous et les approuver. Les plus rusés d’entre eux, les premiers, les tolérants conscients se demanderont quand même, devons-nous permettre de nous effacer le sentiment légitime de vie privée lésé ici parce que les individus pris au dépourvu sont nous, les insignifiants, pour une poignée de criminels.

En ajout, les principaux détenteurs de ces appareils adaptés à la surveillance des réseaux cellulaires sont les mêmes qui écrivent nos lois, ce sont nos élus et leurs organisations, les entreprises d’états, les armées, la police. Ces informations de privilégiés, devraient améliorer les intérêts du peuple, profitons-nous bien plus que, les politiciens peut-être centrés sur leurs intérêts, les commerçants qui connaissent leurs rivaux mieux qu’ils se connaissent eux-même, le marché boursier devenu une terre propice à l’espionnage sans parler de l’espionnage industriel, que notre imagination a tout juste constaté.

Le véritable dommage surviendrait lorsque les inégalités sociales, financières, etc. seraient favorisées par l’utilisation de ces technologies par des complotistes oeuvrants dans le privé ou si l’espionnage international est meilleur du côté de ceux qui ont moins renforci la loi ou s’en servent plus tout court. Les pires irrespectueux de la vie privée du monde seraient avantagés par la disponibilité de leur ressources d’espionnage de communication sans-fil bon marché.

Plusieurs peu scrupuleux personnages, espions de masse, empêcherait la population innovatrice de travailler sur des projets confidentiels en partenariat puisque la plupart des communications se font par voie cellulaire et que nous ne sommes pas assez entrainés. La matière académique, l’information nécessaire pour nous protéger est absente ou mal véhiculée pour contrer cette écoute inappropriée; cela irait de mal en pis si les gouvernements au service des contribuables continueraient d’oeuvrer sans la transparence attendue par la majorité vivante sur les territoires où le pouvoir est démocratique. De plus, au moment où nous approchons le sujet, les entreprises spécialisées méconnues expérimentent déjà les nouveaux avenues en toute catiminie et nous sommes leurs cobayes. Possiblement, leurs cibles seront finalement, hasardeuses pour nous et prolifiques pour eux. La course à l’armement silencieuse qu’est l’espionnage est peut-être déjà à son apogé et nous payons les frais sans le savoir.

**CONCLUSION**

La force nous fait admettre, c’est impossible de faire du cas par cas et surveiller tout le monde qui surveille. Ainsi, des lois sévères devraient interdire mondialement la vente de ces appareils de surveillance au privé sauf sur avis contraire d’une autorité particulière, familière avec la technologie, connue du peuple; la technologie de surveillance des ondes cellulaires oeuvrant dans le respect le plus élevé possible pour la population et peut-être même demander une surveillance externe spéciale de ceux qui ont eux le mandat officiel. En effet, cette idée est la première en concluant car au plus profond de nos esprit, nous savons intimement que ces appareils ne sont pas là pour disparaître, qu’ils existent déjà et rien au monde ne pourrait empêcher le pire malfrat de se les procurer. Comment se protéger le premier venu demandera, et nous lui répondrons, utilises la technologie de chiffrement avancé sur appel voIP, il y a même l’option «vidéoconférence» et le timer de destruction des messages mais ceci sera pour un autre débat génial!

Merci, au plaisir,

Guillaume Blouin

# BIBLIOGRAPHIE

**Articles de journaux en ligne :**

[Martin Untersinger](https://www.lemonde.fr/signataires/martin-untersinger/), MU. (2015, 10 avril). Que sont les IMSI-catchers, ces valises qui espionnent les téléphones portables?. *Le Monde.* Récupéré de https://www.lemonde.fr/pixels/article/2015/03/31/que-sont-les-imsi-catchers-ces-valises-qui-espionnent-les-telephones-portables\_4605827\_4408996.html

**Articles de journaux en ligne :**

Maryse Bernard, MB. (2019, 18 Juin). La police de Vancouver a utilisé le système de surveillance téléphonique StingRay, dit la BCCLA. *Radio-Canada.* Récupéré de <https://ici.radio-canada.ca/nouvelle/796929/espionnage-josh-paterson-association-libertes-civiles>

**Articles de journaux en ligne :**

Inconnu, XX. (2013-07-31). Surveillance électronique de la NSA: après PRISM, XKeyscore. https://ici.radio-canada.ca/nouvelle/625536/xkeyscore-espionnage-snowden-nsa-internet-surveillance

**Articles de journaux en ligne :**

Inconnu, XX. (le 3 septembre 2020). NSA : le programme de surveillance téléphonique révélé par Snowden jugé illégal. https://ici.radio-canada.ca/nouvelle/1731295/edward-snowden-nsa-prism-illegal-loi-jugement-cour

**Page web :**

James Bonta, Suzanne Wallace-Capretta, Jennifer Rooney

(1999, mai). La surveillance électronique au Canada. Dans Sécurité publique Canada.

Récupéré de [https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/lctrnc-mntrng-cnd/index-fr.aspx#\_Toc449846602](https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/lctrnc-mntrng-cnd/index-fr.aspx" \l "_Toc449846602)

**Page web :**

[Martin Ouellet-Diotte](http://ici.exploratv.ca/)

(2020, 20 mai). 5 technologies controversées pour combattre le crime,   
→ Lorsque le StingRay vous écoute.

Récupéré de <https://ici.exploratv.ca/blogue/5-technologies-controverse-science-crime-terrorisme/>

**Page web :**

### [Noa Ouziel](https://www.firstpoint-mg.com/blog/author/noa/)

(January 31, 2020). Top 7 IMSI Catcher Detection Solutions for 2020,

Récupéré de https://www.firstpoint-mg.com/blog/top-7-imsi-catcher-detection-solutions-2020/

**Article wiki :**

IMSI-catcher (30 mai 2021). Dans wikipedia. Récupéré le 5 Juillet 2021 de https://fr.wikipedia.org/wiki/IMSI-catcher