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) 8

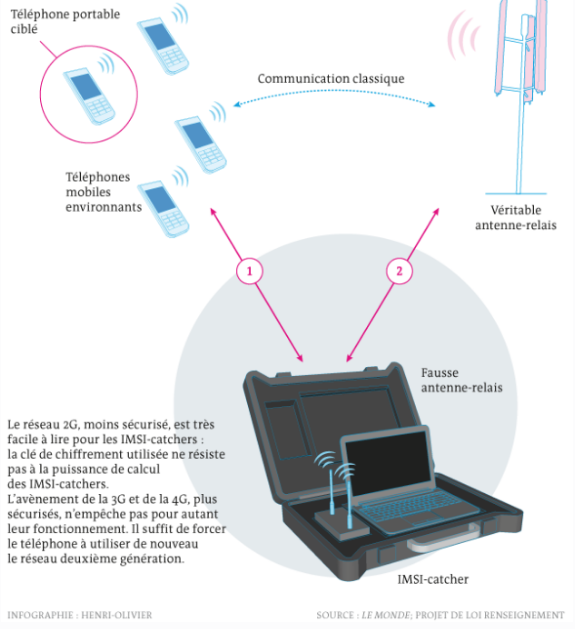
[BIBLIOGRAPHIE](#_Toc53574225) 9

# 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.

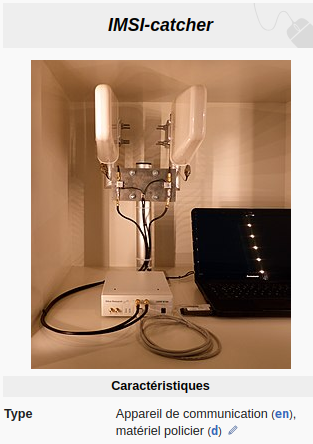


Ce serait intéressant d’en apprendre davantage sur cette fausse antenne pour déterminer si le feu en vaut la chandelle. L’usage de cet appareil peut alimenter les controverses et nous devront y voir plus clair; nous devrons déterminer qui sont les principaux usagers, quels sont leurs objectifs, et où 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 ».



# FONCTIONNALITÉS

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.

## **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](https://www.lemonde.fr/signataires/martin-untersinger/). 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 sans mandat et respect pour les contribuables. Le fait que des révélations soient faites aux moments où des fuites de données surviennent, celles de Snowden par exemple, montre une piètre transparence des autorités par rapport à la divulgation des outils utilisés pour la surveillance autant de masse que ciblées. 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](https://www.lemonde.fr/signataires/martin-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**

Arrêter les méchants devrait être ’une technologie comme celle des surveillances életorniu

# CONCLUSION

Lorem ipsum dolor sit amet, cum ignota nominati ut. Qui discere vivendo ei, mei harum ocurreret et, ei constituto dissentias mei. Verterem constituam ad has, ius veniam dolores ne, eos eu viris hendrerit. Sit id regione tritani omittam, qui ea amet feugait percipit. Id inimicus scriptorem deterruisset vix, disputationi voluptatibus ius et, case mentitum vim ex.

Et periculis philosophia per. Te saepe exerci ancillae eam. His autem porro corpora ex, ne quo assentior definitiones, usu te regione saperet maiestatis. Ad duo illum definiebas, ei vivendum similique nec, cum nisl mucius sadipscing eu. Ad autem melius fuisset has. Ut nulla aliquam eos, inani nobis eos ei, id unum munere prodesset sed. Rebum partem vivendum vis ei. Quot essent singulis qui te. Est id populo labitur, ad usu epicuri facilisi. Autem dicat consequat has te. Impetus invidunt verterem sed at, debet ornatus qui at, et mea dictas aliquip splendide.

# 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

**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/

**Article wiki :**

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