# Un drone qui pirate les smartphones | Denis JACOPINI

10

| | |
|---|---|
|  | **Un drone qui pirate les smartphones** |

**Les drones civils commencent à gagner en popularité, et certains s'inquiètent déjà des atteintes à la vie privée qu'ils pourraient faciliter. Au-delà de la simple surveillance, un spécialiste en sécurité met en avant leur utilisation possible à des fins de piratage de données personnelles.**

Des experts en sécurité de la société Sensepost ont développé un drone capable de pirater le contenu d'un smartphone depuis les airs. Glenn Wilkinson, qui l'a créé en collaboration avec Daniel Cuthbert, se définit comme un hacker consciencieux, et ses recherches ont pour but de pointer du doigt les failles de sécurité des objets connectés, et notamment des smartphones.
Il présente en ce moment ses travaux à la conférence Black Hat qui se tient à Singapour du 25 au 28 mars. La technologie installée sur le drone, baptisée Snoopy, cherche des appareils mobiles dont le Wi-Fi est activé. Il tire parti de la fonction de recherche de réseaux Wi-Fi auxquels l'appareil s'est déjà connecté, qui est intégrée par défaut à tous les smartphones et tablettes. Le drone prétend alors être l'un de ces anciens réseaux déjà connus, et dupe le smartphone (ou la tablette), interceptant toutes les informations qu'il envoie. Il peut de plus se connecter à plusieurs appareils simultanément, usurpant plusieurs réseaux au besoin.
Les informations interceptées vont des sites visités à tous les identifiants utilisés (Amazon, PayPal, etc.) en passant par les coordonnées bancaires, les données de géolocalisation, et d'autres informations critiques, y compris les noms de tous les réseaux auxquels il s'est déjà connecté.
Le site CNNMoney a récemment testé Snoopy avec son concepteur lors d'une virée à Londres. En à peine une heure, ses équipes ont collecté des informations provenant de 150 appareils mobiles. L'utilisation d'un drone rend cette technologie particulièrement impressionnante, car elle permet de suivre des cibles tout en restant hors de portée, pratiquement indétectable.

**Ci-dessous une vidéo du drone en action réalisée par CNN :**

---

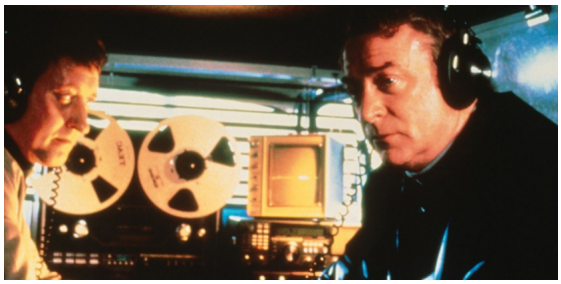


---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.industrie-techno.com/un-drone-qui-pirate-les-smartphones.29240
Par Julien BERGOUNHOUX

# Les 8 techniques les plus ahurissantes des espions d’aujourd’hui | Le Net Expert Informatique



Les 8 techniques les plus ahurissantes des espions d’aujourd’hui

**Un projet de loi entend multiplier les possibilités de surveillance des agents du renseignement français. Tour des outils à disposition des services secrets dans le monde.**Les services de renseignement français vont bientôt voir leurs possibilités d'espionnage multipliées, avec le projet de loi concocté par le gouvernement. L'occasion de faire le point sur l'éventail des outils à disposition des services secrets à travers le monde.

**1. Ecouter les téléphones**
Il s'agit de la pratique la plus évidente : l'écoute des conversations. En France, n'importe quel particulier peut être mis sur écoute dans le cadre d'une affaire portant « sur la sécurité nationale, la prévention du terrorisme, de la criminalité et de la délinquance organisée ».
Cette capacité s'est généralisée (pour atteindre un budget de 43 millions d'euros en 2013) et va parfois très loin. L'agence de renseignement américaine NSA s'est dotée d'une gigantesque capacité d'interception, avec son programme Mystic. En 2011, celui-ci aurait même servi à enregistrer 100% des appels passés dans un pays.
Pour simplifier les interceptions, la NSA a également des millions de données, notamment de Français, en se branchant directement sur le câble sous-marins ou les infrastructures internet par lesquels transitent 99% des télécommunications. L'agence était ainsi capable de récupérer en moyenne chaque jour 3 millions de données concernant des Français (conversations téléphoniques, SMS, historiques de connexions internet, e-mails échangés…).


Une écoute téléphonique dans le film « Le quatrième protocole » de John Mackenzie (1987) (AFP)

**2. Ecouter Skype, Whatsapp et BBM**
Les autorités françaises peuvent mettre en place des écoutes, sur simple décision administrative. Mais cette capacité d'écouter aux portes devrait s'étendre. Le projet de loi souhaite étendre les interceptions également aux SMS et aux e-mails. De plus, un discret amendement au projet de loi Macron va permettre d'étendre les écoutes aux services internet. A terme, les services pourront écouter/lire les conversations sur Skype, Hangout de Google, Whatsapp, WeChat, Line, Facebook Messenger, Viber, BBM, etc.
Microsoft aime à rappeler que, sur son service Skype, deux clefs de chiffrement aléatoires et inconnues de l'entreprise sont créées à chaque conversation, rendant techniquement impossible de brancher des écoutes. Seulement, l'argumentaire a été mis à mal à la suite d'une polémique en 2012 où le site Slate expliquait que des dispositifs techniques avaient été mis en place pour faciliter les interceptions de communication. L'année suivante, le « New York Times » révélait que Skype aidait les forces de l'ordre américaines à accéder aux données de ses clients.

**3. La mallette qui écoute tout**
Si l'écoute classique ne suffit pas, les services peuvent faire appel à une précieuse mallette : l'IMSI-catcher (parfois aussi désignée par sa marque, StingRay). Cet appareil permet de capter et d'enregistrer toutes les communications (appels, SMS) des téléphones à proximité. Techniquement, il se fait passer pour l'antenne de l'opérateur pour faire transiter par son disque dur toutes les conversations. Il suffit alors de se trouver à portée d'un suspect pour l'écouter.
Une solution largement utilisée par les agences de renseignement dans le monde entier. Aux Etats-Unis, pas moins de 46 agences locales dans 18 Etats y ont recours. Il faut dire que l'IMSI-catcher est plus accessible que jamais : il faut compter 1.800 dollars pour acquérir une mallette prête à l'emploi sur internet, selon « Wired ».

Le projet de loi du gouvernement prévoit d'autoriser leur utilisation par les services français, après avoir reçu l'aval d'un juge.
La NSA aurait même poussé le concept d'IMSI-catcher plus loin puisque, selon des documents d'Edward Snowden, la police fédérale américaine (US Marshall) utilise de petits avions de tourisme dotés de la même technologie afin de capter les communications de suspects.

**4. L'aide des hackers**
A l'image de James Bond, les services secrets peuvent utiliser micros et caméras pour surveiller des suspects. Ils peuvent aussi utiliser des balises GPS afin de les géolocaliser « en temps réel ». Des dispositifs que le projet de loi français entend légaliser. Mais il souhaite aller plus loin et permettre l'usage de logiciels espions.

Intitulés « keyloggers », ces logiciels-mouchards permettent de recopier en temps réel tout ce qui se passe sur un ordinateur, un smartphone ou une tablette. La navigation internet, les mots de passe saisis, les fichiers stockés… tout est accessible. Le texte du gouvernement précise que « des agents spécialement habilités » pourront « poser, mettre en œuvre ou retirer les dispositifs de captation ». Concrètement, des hackers des services de renseignement pirateront en toute légalité les machines des suspects pour mieux les espionner.

Issue du monde du piratage informatique, la pratique a fait des émules dans les services de renseignement. La NSA aurait ainsi développé un ver informatique, caché dans les disques durs vendus, capable d'espionner tous les faits et gestes, mais aussi de voler n'importe quel document de dizaine de milliers d'ordinateurs à travers le monde.

Mais la France n'est pas en reste puisque deux rapports indiquent que les services de renseignement hexagonaux ont développé leur propre logiciel malveillant, baptisé « Babar », qui renferme un keylogger. Objectif : écouter les conversations en ligne sur Skype, Yahoo Messenger et MSN, mais aussi de savoir quels sites ont été visités.

**5. Ecouter autour du téléphone, même éteint**
Le téléphone portable est décidément devenu le meilleur ami des agences de renseignement. Outre les écoutes et la géolocalisation, le mobile peut facilement se transformer en micro, même s'il est éteint.

Des documents d'Edward Snowden ont ainsi mis en lumière que la NSA (encore et toujours) est capable d'installer à distance un programme fantôme sur un portable afin de le transformer en espion. Le magazine « Wired » qui rapporte l'information n'entre pas dans les détails, mais ce ver permet de faire croire que l'appareil s'éteint alors qu'il continue de transmettre des informations (sur son contenu notamment). Pour s'en prémunir, la seule solution est de retirer la batterie.

Des hackers ont fait savoir depuis longtemps qu'il est possible de pirater un téléphone et d'en faire un véritable mouchard : écoute des appels, copie des SMS, géolocalisation, écouter les sons environnant (dans un rayon de 5 à 8 mètres), enregistrer la vidéo captée par l'objectif… Et la fonction micro fonctionne même si l'appareil est éteint (mais conserve sa batterie). Une fonction qui a sûrement déjà séduit des agences de renseignement à travers le monde.

6. La carte des interactions humaines
La NSA a aussi un appétit vorace pour les métadonnées. Tous les échanges électroniques (appels, SMS, e-mails, surf sur internet) colportent également des détails sur ceux-ci : qui communique avec qui, à quelle heure, pendant combien de temps, depuis où, etc. Des données qui se rapprochent des fadettes (les factures téléphoniques détaillées) et qui intéressent grandement la NSA.

L'agence a mis en place un programme visant à collecter et à stocker l'ensemble des métadonnées obtenues par les opérateurs télécoms américains. Objectif : constituer une gigantesque base de données permettant, à tout moment, de connaître les interactions entre personnes sur le sol américain. Une idée qui plaît aussi aux renseignements français, déjà experts des fadettes. Le projet de loi souhaite que les autorités puissent avoir accès aux métadonnées d'une personne ciblée sans demander l'avis d'un juge, il suffira d'une autorisation administrative.

Afin de mieux appréhender ce que les métadonnées peuvent dire de nous et de nos interactions, le Massachusetts Institute of Technology (MIT) propose l'outil Immersion qui permet de visualiser sa galaxie de relations basée sur son adresse Gmail de Google.

**7.  La constitution d'une banque de photos**
Toujours selon des documents de Snowden, la NSA collecte chaque jour une quantité astronomique de photos (« des millions d'images ») afin de s'en servir dans le cadre de reconnaissance faciale. Le tout est récupéré dans des e-mails, SMS, sur les réseaux sociaux, via les outils de vidéo-conférences, etc.
Quotidiennement, l'agence obtiendrait 55.000 photos permettant d'identifier des individus, afin d'alimenter une immense banque d'images. L'objectif étant de pouvoir identifier rapidement un suspect, en particulier quand la banque d'images des photos de passeports ne suffit pas.

**8. Fouiner dans les téléchargements illégaux**
Les téléchargements illégaux peuvent aussi aider les autorités, ou du moins les aiguiller. Un document d'Edward Snowden a révélé que les services secrets canadiens ont chaque jour scruté l'ensemble des téléchargements réalisés sur des plateformes comme MegaUpload ou RapidShare, afin de repérer les manuels et documents édités par des groupes terroristes, afin d'identifier leurs auteurs et ceux qui les consultent. Ils produisaient alors une liste de suspects, transmise à leurs alliés, dont les Etats-Unis. En somme, une aiguille dans une botte de 10 à 15 millions de téléchargements quotidiens.

---



---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://tempsreel.nouvelobs.com/tech/20150317.OBS4818/les-8-techniques-les-plus-ahurissantes-des-espions-d-aujourd-hui.html
Par Boris Manenti

# Un oeil sur vous – Citoyens sous surveillance ! Replay jusqu'au 30/03/2015 | Denis JACOPINI

| | |
|---|---|
|  | Un oeil sur vous – Citoyens sous surveillance ! Replay jusqu'au 30/03/2015 |

**Existe-t-il encore un espace dans nos vies citoyennes qui échappe à la surveillance ? Observer, contrôler et analyser les comportements n'ont jamais été aussi aisés qu'aujourd'hui. Depuis une dizaine d'années, les avancées technologiques se sont accélérées, jusqu'à favoriser une révolution sociétale : la surveillance ciblée s'est transformée progressivement en une surveillance de masse à l'échelle planétaire.**

Jadis concentrée sur l'espace public, elle pénètre désormais notre vie privée. L'intimité est une notion de plus en plus floue, soumise à des attaques de moins en moins détectables. Plus sournois que les caméras de surveillance dont beaucoup aimeraient qu'elles couvrent chaque angle mort de l'espace public, le « regard invisible » joue les passe-muraille : jeux vidéo connectés, activité sur les réseaux sociaux, requêtes sur les moteurs de recherche ou géolocalisation via nos smartphones sont autant de constituants manipulables de notre seconde identité – l'alter ego numérique.
En fournissant, souvent sans y consentir ni en avoir conscience, un nombre important de données, le citoyen est devenu l'enjeu d'une bataille politico-économique sans précédent, entre les tenants du tout-sécuritaire, les multinationales du web ou les défenseurs des libertés individuelles.

Emission diffusée sur Arte le mardi 24/03/2015 à 20h50
Rediffusion le mar 07/04/2015 à 8h55
Regardez le replay de l'émission jusqu'au 30/03/2015

---



---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.arte.tv/guide/fr/049883-000/un-oeil-sur-vous-citoyens-sous-surveillance

# Réglementation des drones et droit des robots | Le Net Expert Informatique


source : http://live.orange.com/drones-parrot-amazon-zephyr/

Réglementation des drones et #droit des robots

**Le survol des drones au dessus des centrales nucléaires [1] ainsi que d'autres sites sensibles et parisiens [2]  représente une menace face à laquelle les réponses, notamment réglementaires, semblent encore insuffisantes.**

En effet, la détection par radar militaire mais également l'interception de ces engins volants se révèlent difficiles de par la furtivité des drones et l'incapacité actuelle des autorités à les tracer et à les écarter.

Au niveau réglementaire, l'utilisation des drones ou plus exactement d' « aéronefs qui circulent sans monde à bord » civils, à distinguer des drones militaires, est encadrée par deux arrêtés d'avril 2012 [3], un arrêté relatif aux conditions de navigabilité et de télépilotage et un autre relatif aux exigences liées à l'espace aérien.

**Le principe est le suivant :**
sauf autorisation particulière, les drones doivent survoler un espace bien précis délimité en volume et en temps, en dehors de toute zone peuplée. De plus, en fonction de deux catégories de critères (finalité d'utilisation et poids du drone), des règles particulières s'appliquent. Ainsi, les drones civils professionnels utilisés par exemple par les agriculteurs ou les photographes doivent  notamment se faire connaître auprès des autorités.
Concernant l'utilisation de drone de loisirs qui est en vente libre, il faut également respecter des règles spécifiques qui sont rappelées dans une notice rédigée par la Direction Générale de l'Aviation Civile (DGAC) en décembre 2014 [4] et qui interdisent notamment le vol de nuit, le survol des sites sensibles ainsi que de l'espace public en agglomération.
Au final, la violation des conditions d'utilisation des drones est passible d'un an d'emprisonnement et de 75000 euros d'amende en vertu de l'article L.6232-4 du code des transports.
Autre point d'importance à souligner, même si la prise de vue aérienne est réglementée par l'article D. 133-10 du code de l'aviation civile, il n'en demeure pas moins que la captation et l'enregistrement d'images relatives aux personnes relèvent également de la loi « Informatique et Libertés »[5].
En effet, il est important de souligner également le risque de collecte de données à caractère personnel par les drones. Un facile parallèle peut être établi entre le survol des drones et le passage dans nos rues des « Google cars ».  La CNIL avait constaté lors de contrôles effectués fin 2009 et début 2010 que la société Google, via le déploiement de véhicules enregistrant des vues panoramiques des lieux parcourus, récoltait, en plus de photographies, des données transitant par les réseaux sans fil Wi-Fi de particuliers, et ce à l'insu des personnes concernées. Cette collecte déloyale de très nombreux points d'accès Wi-Fi  constitue un réel manquement à la loi « Informatique et Libertés ».
Concernant les drones, il faudra donc s'attacher à vérifier qu'ils ne récupèrent pas également des données à caractère personnelle de façon illégale. En effet, les drones sont des machines qui peuvent embarquer une quantité importante de capteurs divers et variés tels un appareil photo, une caméra ou un dispositif de géolocalisation permettant de collecter et diffuser des données à caractère personnel avec pour conséquence l'atteinte manifeste à la vie privée des individus.
Consciente de ces enjeux depuis 2012, la CNIL, en liaison avec le Groupe des 29 CNIL européennes (G29) réfléchit activement à l'amélioration de la réglementation à ce sujet.

Au final, la réglementation relative aux drones qui, d'une part, a le mérite d'exister et, d'autre part, est relativement souple et adaptable en prévoyant plusieurs scénarii spécifiques, apparaît même novatrice au niveau international. Les Etats Unis par l'intermédiaire de la Federal Aviation Association (FAA) n'ont dévoilé que le 15 février 2015 et pour la première fois des recommandations pour encadrer l'utilisation des drones civils commerciaux sur le sol américain [6].
Toutefois, la DGAC a prévu quand même de réviser prochainement la réglementation des drones afin de mieux prendre en compte la massification de l'utilisation de drones civils. Cette révision devra si possible prendre en compte une future réglementation européenne à ce sujet.

Plus largement, ce focus juridique sur les drones peut élargir son horizon en s'intéressant à la problématique du droit des robots qui, au regard de la vitesse de création des inventions technologiques, constitue indéniablement un des enjeux majeurs juridiques mais également éthiques des années à venir.
Certes pour les objets connectés, les enjeux juridiques ont déjà été identifiés mais il semble qu'il faille pousser le cadre juridique plus loin pour les futures générations de robot doté d'une certaine forme d'intelligence artificielle.
La vente du robot, comme tout bien, entraine pour le vendeur une obligation de garantie et engage sa responsabilité délictuelle du fait d'un défaut de sécurité de l'un de ses produits ou services entraînant un dommage à une personne. Cependant, il est probable que l'autonomie des robots grandissante, il faille réfléchir à la responsabilité propre du robot. De prime abord, la responsabilité juridique repose sur la notion de discernement, actuellement les machines restent sous la responsabilité de son gardien soit de l'usager ou encore de son fabricant par le biais de la responsabilité des produits défectueux.
Il est possible que, dans un futur plus ou moins proche, le législateur décide de mettre en place une personnalité juridique spécifique du robot. Cette dernière, se distinguant du régime juridique lié aux animaux et des biens, devra être encadrée afin de prévoir la sécurité des utilisateurs mais également la sécurité du robot lui-même. Pour commencer, il pourrait même s'agir de la reprise des trois règles de la robotique édictée par Isaac Asimov [7]!

[1] Dix-sept centrales nucléaires sur les dix-neuf que compte le parc français ont été survolées par des drones depuis début octobre. Six l'ont été simultanément dans la nuit du 31 octobre.
[2] http://www.liberation.fr/societe/2015/02/24/paris-survole-par-des-ovnis_1209273
[3]Les arrêtés du 11 avril 2012 relatifs d'une part à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et d'autre part à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent constituent le socle réglementaire d'utilisation des drones civils.
[4] Règles d'usage d'un drone de loisir :  http://www.developpement-durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf
[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.
[6] « Drones civils – les Etats-Unis avancent sur leur législation : les différences avec le modèle français  » par Emmanuel de Maistre, président de Redbird : http://www.infodsi.com/articles/154099/drones-civils-etats-unis-avancent-legislation-differences-modele-francais-emmanuel-maistre-president-redbird.html?key=a0a42d0bc78aa63d
[7] http://nte.mines-albi.fr/SystemiqueSudoku/co/v_regle_vie_Azimov.html

---



---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://securitedessystemesjuridiques.blogspot.fr/2015/03/reglementation-des-drones-et-droit-des.html

---

# Géolocalisation : tous

# traqués ? Emission du 12 février 2015 à voir ou à revoir | Le Net Expert Informatique

## Géolocalisation : tous traqués ? Emission du 12 février 2015 à voir ou à revoir

**Les Français utilisent leur portable près de 170 fois par jour. Mais ils font bien plus que téléphoner. Ils prennent des photos, vont sur les réseaux sociaux, se déplacent… tout en se géolocalisant. Pour Envoyé spécial, une équipe a rencontré plusieurs adeptes de ce procédé.**

Grâce à la puce GPS de leur smartphone, ils peuvent trouver la boulangerie ou le cinéma le plus proche, calculer leur trajet en voiture ou en bus, repérer les embouteillages… Plus surprenant : ils peuvent aussi suivre leurs amis à la trace, draguer des passant(e)s, payer leur prime d'assurance de voiture moins cher et même… gagner de l'argent en faisant leurs courses ! Tout ça grâce à des applications de géolocalisation qui se téléchargent en un clic sur leur téléphone.
Mais à force de dire en permanence où nous sommes, notre portable est devenu un véritable mouchard, capable de nous traquer à notre insu… Une aubaine pour les publicitaires, les géants du net, et même les enseignes – qui peuvent cibler le contenu qu'ils vous envoient.
La géolocalisation est désormais une arme commerciale redoutable. Envoyé spécial a enquêté sur ce phénomène mondial qui menace notre vie privée.

---



---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.francetvinfo.fr/replay-magazine/france-2/envoye-special/envoye-special-du-jeudi-12-fevrier-2015_822079.html

---

# 50 000 chauffeurs d'Uber

# victimes d’une attaque informatique | Le Net Expert Informatique

| | |
|---|---|
|  | 50 000 chauffeurs d’Uber victimes d’une attaque informatique |