

ANR-14-CE28-0024-02
Programme « UTIC France-Europe »



Capacités d'interception et de surveillance. L'évolution des systèmes techniques

Philippe Guillot (Univ. Paris 8), Daniel Ventre (CNRS, laboratoire CESDIP)



Livrable n° 1

Version du 06/01/2019

Table des matières

I - Introduction.....	5
Contexte	5
L'objectif du rapport.....	6
Les grandes lignes de l'étude	6
Un rappel historique, chronologique, contextuel	6
Les techniques, technologies et capacités	6
Les enjeux du chiffrage.....	7
Le droit.....	7
II - Historique	7
2.1. Les cabinets noirs	7
2.2. Echelon	8
2.3. Les années 2000-2010.....	10
III - Définitions	10
3.1. L'interception	11
3.1.1. Interception.....	11
3.1.1.2. L'Interception est-elle intrusion ?	13
3.1.2. Interception légale	13
3.1.3. Interception stratégique, interception tactique	14
3.1.4. Interception ciblée (targeted) et interception massive (bulk)	15
3.1.5. Interception passive, interception active	17
3.2. La surveillance	17
3.3. Les données.....	18
3.3.1. Le signal physique.....	18
3.3.2. La donnée brute	19
3.3.3. Les données interprétées	19
3.3.4. Les métadonnées	19
IV – Méthodes, techniques et technologies de cybersurveillance/interception	21
4.1. Pour une typologie des technologies d'interception et de cybersurveillance	22
4.2. Techniques, technologies, méthodes et dispositifs d'interception	24
4.2.1. Différentes méthodes d'interception.....	24
4.2.1.1. Interception à la source.....	24
4.2.1.2. Interception pendant la transmission	25

4.2.1.3. Les interceptions téléphoniques	25
4.2.1.4. Les interceptions radio	26
4.2.1.5. Les communications numériques.....	26
4.2.1.6. L' « interception » pour la gestion des réseaux locaux	27
4.2.2. De l'analyse de trafic à l'exploitation des métadonnées	27
4.2.3. Intégrer les équipements d'interception à la source même des infrastructures/architectures de télécommunication.....	28
4.2.4. « Man-In-The-Middle » (MITM)	31
4.2.5. Le DPI (Deep Packet Inspection).....	32
4.2.6. Les IMSI-Catcher	33
4.2.7. Les portes dérobées (backdoors)	33
4.3. Surveiller les e-mails.....	38
4.4. Les messageries sécurisées	39
4.4.1. MinInt(F) versus messageries sécurisées	40
4.4.2. BlackBerry, l'application BBM et les Etats.....	40
4.5. L'interception des communications dans les lieux publics	43
4.6. Internet, un réseau de câbles.....	43
V – Protéger les communications contre les risques d'interception	45
5.1 - La cryptographie.....	45
5.2 - La stéganographie	46
5.3. - Le calcul quantique.....	48
5.4 - La cryptographie quantique	48
VI – Le droit, ses objets, ses évolutions.....	49
6.1. Origines et Evolution de la réglementation en cryptologie	49
6.1.1. Le développement du télégraphe	49
6.1.1.1. Le télégraphe optique de Chappe	49
6.1.1.2. Le télégraphe électrique.....	50
6.1.2. Depuis la deuxième guerre mondiale.....	50
6.1.2.1. Aux États-Unis	51
6.1.2.2. En France : les tiers de confiance	52
6.2. Les arrangements de Wassenaar	52
VII - Conclusion	54
VIII – Bibliographie complémentaire.....	56
8.1. Ouvrages, articles (par ordre chronologique)	56

8.2. Autres rapports et études d'organisations et institutions (par ordre chronologique) 56

I - Introduction

L'évocation des pratiques de cybersurveillance et d'interception des télécommunications renvoie à des débats récents (les divulgations d'Edward Snowden datent de juin 2013) ou plus anciens (les révélations et les rapports européens sur le programme Echelon datent quant à eux de la deuxième moitié des années 1990¹). Un volume très important d'articles a été produit sur ces deux temps forts de l'histoire controversée de la surveillance et des pratiques en matière d'interception. Controversée, parce que même lorsqu'elles sont légales, légitimes, justifiées, l'interception et la surveillance suscitent des interrogations sur les limites des pratiques, sur leurs modalités, et des craintes de dérapages, d'abus, d'atteintes à des droits fondamentaux, à des libertés. Avec les pratiques de surveillance et d'interception, il est possible d'exercer un contrôle sur les individus, sur des groupes, des sociétés, même si les objectifs sont louables et nécessaires (lutte contre le crime, contre le terrorisme, assurer la sécurité, le développement économique, etc.) Pratiques controversées enfin car rien ne garantit que les résultats poursuivis et motivant ces pratiques de surveillance, soient atteints effectivement, ni que leur mise en œuvre ne soit détournée de l'objectif initial (surveillance d'opposants politiques, à des fins personnelles, ou encore de distorsion de concurrence économique).

Contexte

L'évocation des pratiques de cybersurveillance et d'interception des télécommunications renvoie aux diverses controverses qui ont émergé ces dernières décennies : tout d'abord suite aux révélations des pratiques d'interception des communications satellitaires par les Américains et leurs alliés dans les années 1990 (programme Echelon et réactions européennes), puis à celles d'Edward Snowden venues mettre en lumière l'ampleur des opérations conduites par les renseignements américains mais également de nombreux autres Etats pour tirer parti des nouvelles capacités offertes par internet et plus largement par l'ensemble des nouvelles technologies d'information et de communication. Ce mois-ci, mars 2017, la publication par le site WikiLeaks d'un nouvel ensemble de documents exfiltrés de la CIA, relance les débats sur les pratiques des renseignements. Il ne s'agit plus tant de montrer des capacités d'interception massive (objet central des révélations d'E. Snowden), que de comprendre les méthodes d'interception, de collecte de données, de cybersurveillance ciblées, par l'exploitation de l'internet des objets et des technologies les plus récentes. Les interceptions se font là plus précises, plus intrusives, plus individualisées (exploiter la caméra ou le micro qui est intégré dans un téléviseur connecté et intelligent par exemple ; prendre la main à distance sur un véhicule connecté ou sur des téléphones portables et autres tablettes, pour ne citer là que quelques exemples des multiples capacités techniques déployées, avec ou sans la contribution des constructeurs eux-mêmes). Le buisson de programmes ou projets de la NSA, dans le cas des pratiques d'interception et collecte de données massives, trouve son équivalent dans le champ des interceptions et collectes ciblées de la CIA.

Dans tous les cas ces révélations alimentent des controverses autour de la légitimité des pratiques des agences étatiques, des menaces aux libertés individuelles, aux droits fondamentaux et à la démocratie ; autour des rapports de force ou de coopération, entre acteurs étatiques et privés (industriels, citoyens), civils et militaires ; ou bien encore des débats sur la nature des relations internationales, sur la coopération internationale, etc.

La compréhension des techniques, des technologies, des capacités, ressources, moyens utilisés, déployés, développés, demeure essentielle dans ces divers débats. Car il ne saurait y avoir de mesure saine des enjeux sans évaluation ou compréhension, ne serait-ce qu'*a minima*, des possibilités.

¹. Cf. Sébastien-Yves Laurent, *Atlas du renseignement. Géopolitique du pouvoir*, Paris, Presses de Sciences-Po, 2014, 190 p.

L'objectif du rapport

L'objectif de ce premier rapport du projet UTIC est de proposer une grille de lecture des aspects techniques ou technologiques des capacités d'interception. Ce rapport est donc essentiellement conçu comme un outil de travail pour les chercheurs qui contribueront à la suite du projet UTIC. Il s'attachera à :

- rappeler les définitions de concepts essentiels au projet (surveillance, interception, données, etc.)
- décrire des techniques, méthodes, technologies d'interception
- rappeler quelques jalons de l'évolution juridique dans le champ de la cybersurveillance/interception des communications

Sur le plan méthodologique, notre démarche s'appuie sur l'exploitation d'une littérature abondante, partagée entre articles scientifiques, rapports et études des administrations ou du secteur privé, sites internet de présentations d'entreprises, etc.

Les grandes lignes de l'étude

Ce livrable traite des capacités d'interception et surveillance en proposant un panorama large des techniques, technologies, acteurs de l'interception.

Un rappel historique, chronologique, contextuel

Un regard sur le passé s'impose. Les pratiques actuelles de cybersurveillance, interception, collecte des données, s'inscrivent dans une continuité : celle de l'histoire de l'interception, des progrès de la science et de la technologie, de la cryptographie, des technologies de communication (du télégraphe au 19^e siècle, aux réseaux téléphoniques, aux communications satellitaires, à l'avènement de l'internet). Quelles que soient les technologies de communication déployées, les efforts pour intercepter les communications, les échanges, flux, signaux, données, sont une constante de l'activité des Etats en particulier. Plusieurs affaires, révélations, ont émaillé le cours de l'histoire récente, mais n'ont jamais mis un terme aux pratiques, qui n'ont au contraire jamais cessé d'évoluer, de s'adapter aux nouvelles conditions et des nouveaux enjeux. L'interception des communications a dû faire face aux changements d'échelle et de nature qu'a constitué le passage de l'analogique au numérique, avec l'avènement d'internet et de l'informatisation des échanges.

Les techniques, technologies et capacités

Sur le plan technologique les capacités en matière de surveillance/interception ne cessent de progresser, de s'adapter aux évolutions de l'environnement technologique (expansion du cyberspace avec la multiplication des équipements - objets connectés - ou des applications - les messageries sécurisées par exemple). Le nombre de programmes ou projets développés par la NSA ou la CIA, par les agences de renseignement du monde entier, sont le reflet de cette adaptation nécessaire et continue. L'inventaire des catalogues des entreprises offrant des technologies et services d'interception donnent le sentiment que tout, ou presque, est possible en matière d'interception. Plusieurs points sont abordés dans le rapport :

- Quelles sont les différentes catégories et méthodes d'interception ? Peut-on définir une typologie des techniques et technologies de cybersurveillance et d'interception ? Qu'est-ce qu'une porte dérobée ? Un Imsi-Catcher ? Le DPI ? Une messagerie sécurisée ?
- Quelles sont les différentes catégories de données objets de l'interception
- Le chiffrement est-il à lui seul une garantie de protection des échanges et des messages ?

Les enjeux du chiffrement

La généralisation du chiffrement des communications a été rendu nécessaire pour assurer la "confiance dans l'économie numérique".

Il a aussi posé de nouveaux problèmes aux services d'interception en retardant ou en interdisant l'accès au contenu des messages.

Ces problèmes ont connu de solutions variées et maintenu un clivage entre les partisans de la protection de la vie privée et les agences étatiques qui arguent du besoin d'un contrôle pour assurer la mission de lutte contre les organisations mafieuses et terroristes.

L'exploration de l'histoire des techniques cryptographiques permet d'éclairer la situation actuelle et les nombreuses interrogations suscitées par les révélations sur les activités de l'agence de sécurité nationale étasunienne.

La cryptologie rassemble les techniques de protection des informations transmises ou stockées des écoutes ou des modifications malveillantes. Sa maturité est aujourd'hui suffisante pour que son utilisation puisse prétendre conduire à un niveau de confiance acceptable. Les protocoles sont aujourd'hui assortis de preuves de sécurité. Mais ce domaine est en permanente évolution. Les procédés subissent des attaques mathématiques qui mettent en évidence des faiblesses. Certains algorithmes deviennent obsolètes, comme la fonction de hachage MD5, et très récemment SHA1, utilisée pour les signatures numériques, ou encore l'algorithme de chiffrement RC4 utilisé dans certaines normes de protection des réseaux Wifi.

Mais les principales faiblesses résident dans une implémentation défectueuse qui rend la protection inefficace. Des failles sont régulièrement révélées jusqu'à constituer un marché. De plus, les interventions des agences étatiques sur la constitution des normes suscitent des soupçons sur l'existence de portes dérobées (backdoors) qui rendraient les mesures de protection transparentes.

Nous répondrons aux questions posées par la cryptologie en nous concentrant sur son utilisation dans le contexte des interceptions : ce qu'elle protège ou ne protège pas, quel niveau de confiance elle peut prétendre assurer, comment elle peut être contrôlée ou contournée, en quoi les avancées récentes comme les blockchains ou les technologies quantiques peuvent bouleverser ses modalités d'application.

Le droit

Le cadre juridique qui nous paraît essentiel est celui des Arrangements de Wassenaar. Récemment révisés sur proposition de l'Europe, les Arrangements règlementent le commerce des technologies duales. En relèvent à ce titre des solutions de chiffrement, mais aussi les technologies d'interception, de DPI, qui peuvent à la fois servir des usages civils et militaires, légaux ou se transformer en outils de surveillance et de dictature.

L'encadrement juridique des interceptions a dû gérer la transition des télécommunications analogiques (filaires, hertziennes) au numérique, en adaptant les cadres préexistants au nouveau contexte de l'internet.

II - Historique

2.1. Les cabinets noirs

On désigne sous ce terme des officines secrètes, placées sous le contrôle des États sous l'ancien régime, et qui existaient dans la plupart des pays européens. Ces services étaient en charge de

l'interception du courrier postal et de la cryptographie afin de « repérer et censurer les opposants politiques, et s'informer des courriers diplomatiques ou militaires »².

En France, ces cabinets existent dès l'apparition du service postal. L'édit de Louis XI du 19 juin 1464 spécifie dans ses articles 13 et 14 que :

« Les courriers et messagers seront visitez par les commis du grand maistre auxquels ils seront tenus d'exhiber leurs lettres pour connoistre s'il y a rien qui porte préjudice au service du Roy et qui contrevienne à ses édits et ordonnances »³.

Ces cabinets se sont particulièrement développés sous Louis XV, ou un *Cabinet du secret des postes*, recevait l'ordre du surintendant des postes d'ouvrir certains paquets. Ce services, décachetaient les lettres, reconstituaient les cachait et transmettaient les copies au lieutenant général de police et au ministre des affaires étrangères.

En 1789, de nombreux cahiers de doléances réclament l'abolition des cabinets noirs⁴. L'assemblée constituante et la convention proclament l'inviolabilité des correspondances, mais le cabinet noir est rétabli par le Directoire, limitant la surveillance aux lettres étrangères. Il est maintenu sous l'Empire, la Restauration et perdurera jusqu'au second Empire⁵.

2.2. Echelon

Le réseau *Echelon*⁶ est un système mis en place par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle Zélande pour intercepter les communications des satellites commerciaux. Il voit son origine en 1943 dans l'accord UK/USA pendant la seconde guerre mondiale, puis se développe et s'étend aux autres partenaires pendant la guerre froide pour opérer une interception massive dont l'existence est révélée au public à partir des années 1990⁷. Il a contribué à des actions de renseignement économique pour donner un avantage compétitif aux entreprises américaines. La perte par Thomson-CSF au profit de l'américain Raytheon de l'appel d'offre du Brésil pour un système de radars est attribuable aux interceptions Echelon.

Duncan Campbell⁸ publia en 1988 un article dans la revue *New Statesman*, qui mit sur le devant de la scène le programme Echelon. Le Parlement Européen publia à la fin des années 1990 des rapports sur le sujet : le rapport du STOA (Bureau d'Évaluation des Options Techniques et Scientifiques) de 1997, rapport « Interception Capabilities 2000 » qui traite des systèmes d'espionnage des satellites commerciaux et surtout le rapport Schmid qui est un document sans concession, présenté devant le

² https://fr.wikipedia.org/wiki/Cabinet_noir

³ <http://www.cosmovisions.com/Cabinet-Noir.htm>

⁴⁴. Cf. Sébastien-Yves Laurent (dir.), *Le secret de l'Etat - Surveiller, protéger, informer XVIIe-XXe siècle*, Paris, Nouveau monde éditions, 2015, 224 p.

⁵. Cf. Sébastien-Yves Laurent, *Politiques de l'ombre. État, renseignement et surveillance en France*, Paris, Fayard, 2009, 692 p.

⁶ <https://fr.wikipedia.org/wiki/Echelon>

⁷. Cf. Olivier Forcade et Sébastien Laurent, *Secrets d'État. Pouvoirs et renseignement dans le monde contemporain*, Paris, Colin, 2005, 238 p.

⁸ Duncan Campbell est un journaliste d'investigation britannique, qui a révélé au grand public en 1988 l'existence du réseau Echelon, dans un article intitulé *Somebody's Listening*. L'article est disponible à l'adresse suivante : http://new.duncan.gn.apc.org/menu/journalism/newstatesman/Somebody's_Listening.pdf

Parlement européen⁹. De *Surveillance Electronique Planétaire* publié en 2000 par D. Campbell, sur la base du rapport précité, retenons les points suivants :

- des dizaines d'entreprises de la Silicon Valley fournissent les technologies SIGINT à la NSA (entreprises telles que Lockheed Martin, TRW, Raytheon, etc.
- certaines des entreprises qui fournissent les capacités sigint et comint sont dirigées par d'anciens hauts gradés de la NSA
- les communications internationales venant du, et dirigées vers, le Royaume-Uni et les Etats-Unis, sont interceptées depuis le début des années 1920. Au Royaume-Uni une loi de 1920 sur les secrets officiels assure l'accès à tous les types de communication. D'autres lois ont suivi comme la loi de 1984 sur l'interception des communications au Royaume-Uni. Les autres pays participant à Echelon se sont dotés de loi créant obligations pesant sur les opérateurs de télécommunications.
- avant 1970 est l'ère des technologies analogiques. L'après 1990 est essentiellement digital
- Comint : l'accès aux données/messages se fait soit « avec la complicité des opérateurs des réseaux », soit « à leur insu »¹⁰.
- les communications internationales sont systématiquement interceptée, y compris les messages envoyés par ou à des citoyens américains.
- interception d'internet : « depuis le début des années 1990, des systèmes Comint rapides et sophistiqués ont été développés afin de collecter, filtrer et analyser les types de communication digitales rapides utilisés par Internet »¹¹. « L'accès aux systèmes de communication a des chances de demeurer clandestin, tandis que l'accès aux centraux internet risque d'être plus facilement détectable, mais assure un accès plus aisé à davantage de données et des méthodes de tri plus simples »¹².
- à partir de 2000 la tâche d'interception est compliquée par le glissement des télécoms vers les réseaux de fibre optique. « Un accès physique au câble est nécessaire pour l'interception »¹³.

L'accélération de la mise en réseau du monde, depuis le début des années 1990, se traduit par une croissance de la dépendance des sociétés modernes au cyberspace.

Durant la Guerre Froide, la NSA dont la fonction première est l'analyse de signal (sigint) a concentré ses activités sur l'interception passive des transmissions non câblées (« over-the-air ») (exemple : satellites). Internet a changé le jeu. On passe de communications analogiques à des communications numériques, des réseaux numériques. L'interception conventionnelle devient obsolète avec les câbles optiques, et l'expansion des réseaux internet dans le monde rend caduque l'interception telle qu'elle se pratiquait « avant ». Les interceptions doivent être désormais faites au plus près de la source, en ayant accès physiquement aux équipements de transmission. Il y a eu d'autre part changement d'échelle : augmentation considérable du volume des communications, appelant en parallèle un développement des capacités de surveillance. Les Etats-Unis étant au cœur des réseaux de l'internet mondial, la NSA dispose de ce point de vue d'un avantage considérable¹⁴.

⁹. Gerhard Schmid, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques, système d'interception ECHELON (2001/2098 (INI), Rapport A5-0264/2001, Parlement européen, 11 juillet 2001, 210 p.*

¹⁰ page 36. Duncan Campbell, *Surveillance Electronique Planétaire, 2000*

¹¹ page 90. Duncan Campbell, *Surveillance Electronique Planétaire, 2000*

¹² page 61. Duncan Campbell, *Surveillance Electronique Planétaire, 2000*

¹³ page 111. Duncan Campbell, *Surveillance Electronique Planétaire, 2000*

¹⁴ Andrew Clement, *NSA Surveillance: Exploring the Geographies of Internet Interception*, iConference 2014, 14 pages, <https://pdfs.semanticscholar.org/cd2b/02b410a123f5314ebe3fd07d52ece5e3a3c8.pdf>

2.3. Les années 2000-2010

Les attentats du 11 septembre 2001 semblent être un point de rupture dans la culture de la NSA. « *Ex-NSA Analyst J. Kirk Wiebe recalls: "everything changed at the NSA after the attacks on September 11. The prior approach focused on complying with the Foreign Intelligence Surveillance Act ("FISA"). The post-September 11 approach was that NSA could circumvent federal statutes and the Constitution as long as there was some visceral connection to looking for terrorists." While another ex-NSA analyst also remembers: "The individual liberties preserved in the US Constitution were no longer a consideration [at the NSA]."*¹⁵ Mais cette lecture peut être remise en cause. La NSA pratiquait la surveillance élargie aux citoyens américains avant les attentats du 11 septembre ainsi que l'atteste la grande crise publique du renseignement des Etats-Unis tout au long de l'année 1975 qui s'était traduite par un conflit sans précédent entre le Congrès, la Maison Blanche et les agences à la suite des révélations par la presse des activités de la CIA et du FBI¹⁶. "*October 31, 2001: A number of whistleblowers reveal the extent of the NSA's surveillance of the communications of U.S. citizens*"¹⁷. William Binney et J. Kirk Wiebe démissionnent de la NSA et dénoncent les dérives des activités qui y sont menées, notamment au travers du programme *Thin Thread* qu'ils ont contribué à développer au sein de l'agence. Binnet et Wiebe dénonceront ensuite l'existence du programme *Stellar Wind*, qui intercepte les communications à l'intérieur du pays (téléphonie, emails).

Les divulgations de documents classifiés par E. Snowden ont mis en évidence l'existence de pratiques et de capacités de la NSA en matière de cybersurveillance à une échelle massive. Les pratiques sont inscrites dans le long terme, et touchent désormais les citoyens, des civils, des individus, contrairement aux programmes d'interception des communications satellitaires qui pouvaient être dénoncés dans les années 1990 et concernaient avant tout les Etats, les entreprises. Les questions d'alors étaient plutôt celles de l'espionnage économique, de la concurrence déloyale, de l'espionnage politique, etc. Echelon traduisait la recherche de puissance d'un Etat. Les pratiques dénoncées par Snowden traduisent toujours la stratégie de puissance de l'Amérique, mais s'inscrivent surtout dans la politique sécuritaire, dans la lutte ou guerre contre le terrorisme et font selon Snowden naître des risques pour les citoyens. Internet et les diverses applications qui se sont développées depuis le début des années 1990 dans le monde ont ouvert aux agences de renseignement de nouvelles opportunités en matière de collecte et d'accès aux données, en matière d'interception des échanges.

Le rapport « *Interception Capabilities 2014* »¹⁸ différencie les anciennes modalités de l'interception des nouvelles. Les anciennes sont caractérisées par : le modèle de l'interception légale l'interception ciblée, la cause, la proportionnalité, l'exception sécuritaire européenne. Les nouvelles sont caractérisées par : l'échelle, le niveau de profondeur, la multiplicité des méthodes, les partenariats secrets, les attaques illicites, la compromission des matériels.

III - Définitions

Dans les pages qui suivent nous comparons plusieurs définitions des quelques termes essentiels à notre projet : interception (intercepter), surveillance (surveiller), cybersurveillance, données (et ses déclinaisons en donnée numérique, données brutes, métadonnées notamment). L'objectif de cette observation des définitions est de mettre en avant les traits caractéristiques de chacun des objets

¹⁵ Cité dans "Timeline of NSA Domestic Spying", <https://www.eff.org/fr/nsa-spying/timeline>

¹⁶ Cf. Sébastien-Yves Laurent, *Atlas du renseignement. Géopolitique du pouvoir*, Paris, Presses de Sciences-Po, 2014, 190 p.

¹⁷ "The National Security Agency (NSA) Controversy: timeline", site consulté le 1^o mars 2017, <http://www.discoverthenetworks.org/viewSubCategory.asp?id=1933>

¹⁸ <http://www.duncancampbell.org/PDF/CoECultureCommittee1Oct2013.pdf>

traités et de s'interroger sur les limites de ces derniers : par exemple, l'interception peut-elle être confondue avec la cybersurveillance ? L'interception est-elle « intrusion » ?

3.1. L'interception

3.1.1. Interception

L'interception repose sur quelques principes essentiels :

- il doit y avoir flux, déplacement, mouvement (soit d'un objet, soit d'une personne)
- ce flux doit aller d'un point A à un point B
- il doit y avoir une origine et un destinataire ou un lieu d'arrivée voulus, désignés
- l'interception consiste à prendre au passage... le message, l'objet
- il y a ensuite deux acceptions : soit l'interception implique que l'objet ou la personne n'est arrêté que temporairement ; soit elle implique que l'objet ou la personne est empêché d'arriver à son point de destination (« Interrompre la progression de quelqu'un ou de quelque chose » définition du CNRTL)
- l'interception est présentée comme une intrusion car les acteurs qui interceptent sont des tiers, non invités à l'échange : « Enlever, dérober au passage ce qui est destiné à quelqu'un d'autre » (définition du CNRTL). Le message ne leur est pas destiné.
- peut alors se poser la question, juridique, de savoir si l'interception s'apparente à un vol (vol de données).

Terme	Définition	Source
Intercepter	Enlever, dérober au passage ce qui est destiné à quelqu'un d'autre. <i>Intercepter une lettre, un paquet.</i> Prendre connaissance de ce qui est adressé à quelqu'un d'autre. Interrompre la progression de quelqu'un ou de quelque chose.	cnrtl
Intercepter	Arrêter quelque chose au passage, en interrompre le cours direct Prendre connaissance de quelque chose qui ne vous était pas destiné : Intercepter une lettre.	Larousse
Interception	Action de prendre quelque chose au passage, de le détourner de sa destination Action de prendre connaissance d'une conversation, d'un message destiné à autrui. Action d'arrêter la diffusion de quelque chose, la progression de quelqu'un.	cnrtl
Interception	Action d'intercepter ; fait d'être intercepté : L'interception d'une lettre.	Larousse

L'interception est caractérisée par les traits suivants :

- il doit y avoir échange de données, transmission (ce qui permet d'écarter du champ de l'interception toutes les pratiques d'intrusion qui vont aller fouiller les disques durs, les serveurs, s'introduire dans les systèmes pour voler les données, les fichiers stockés). Il n'y a pas interception si la captation intervient avant que les données ne soient envoyées ou après qu'elles aient été réceptionnées. S'introduire dans les fichiers de stockage des emails n'est pas interception.
- L'interception peut être définie comme une **composante de la surveillance des communications**. Interception et surveillance ne sont donc pas synonymes. L'interception se distingue du filtrage de l'internet.

- Lorsqu'elle accède aux contenus, l'interception est une **atteinte au secret des correspondances et à la vie privée**¹⁹
- L'interception est une **capacité au service du renseignement mais avant tout un outil d'enquête policière**
- l'interception n'a d'intérêt que dans la mesure où émetteur et récepteur du message ignorent qu'il y a interception (cette condition devra être discutée. En effet, l'avant et après D. Campbell, l'avant et après Snowden devraient avoir changé le contexte et compliqué la pratique des interceptions, aussi bien ciblées que massives. La société ayant connaissance de l'existence de ces pratiques, des possibilités techniques existantes, ayant été sensibilisée
- médiatisation du réseau échelon, des interceptions de la NSA et des Etats par E. Snowden
- des tactiques ou stratégies de résistance se sont développées. L'interception doit donc intégrer cette nouvelle contrainte: d'une ignorance ou absence de conscience, laissant le champ libre à la surveillance, on est passé à une période de conscience, et de résistance des cibles).
- l'interception consiste à écouter, enregistrer, copier. Nous devons reconsidérer ces actions dans le champ numérique où la notion de « copie » se fait sans aucune altération du message original ; mais où les volumes de données sont un défi central (dans le cas de l'interception de masse, est-il possible de tout « copier », ce qui implique de « stocker » ?)
- les messages, les données, sont interceptés intégralement ou partiellement. Nous devons revenir sur cette question également. La notion de « métadonnées » permet de faire l'économie d'une interception de l'intégralité des messages, quand bien même celle-ci serait possible.
- L'interception prend deux formes : **soit elle concerne les contenus, soit elle concerne les données de communication (métadonnées).**

Nous nous limiterons aux interceptions des communications électroniques, et retiendrons pour notre étude la définition très large proposée dans un rapport publié par l'UIT en 2013²⁰ :

« Conformément au Toolkit for Cybercrime Legislation de l'UIT²¹, l'«interception» désigne «l'acquisition, la visualisation, la capture ou la copie du contenu ou d'une partie du contenu d'une communication, notamment les données relatives au contenu, les données informatiques, les données relatives au trafic, et/ou les émissions électroniques de ces données, par des moyens avec fils, sans fils, électroniques, optiques, magnétiques, oraux, ou d'autres moyens, pendant la transmission grâce à l'utilisation d'un dispositif électronique, mécanique, optique, à ondes, électromécanique, ou un autre type de dispositif²²».

¹⁹ Pour le détail de ces aspects juridiques cruciaux dans le cadre d'UTIC nous renvoyons au futur livrable 7.

²⁰ UIT, Bureau de développement des télécommunications (BDT), « Interception de communications : modèles de lignes directrices politiques et de textes législatifs », Rapport HIPCAR (Harmonisation des politiques, législations et procédures réglementaires en matière de TIC dans les Caraïbes), Genève, 2013, 78 pages, http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/FRENCH%20DOCS/interception_of_communication_mpg-fr.pdf

²¹ UIT, « IUT Toolkit for cybercrime legislation », Genève, février 2010, 69 pages, <http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf>

²² Partie 1 – Définitions, article « k »

3.1.1.2. L'Interception est-elle intrusion ?

Les deux mots ont des sens différents mais parfois l'interception nécessite une intrusion.

Intrusion	<ul style="list-style-type: none">- Fait de s'introduire de façon inopportune dans un groupe, un milieu, sans y être invité : Son intrusion dans l'assemblée causa une grande gêne.- Fait d'intervenir dans un domaine où il ne conviendrait pas de le faire : L'intrusion de la politique dans le sport.- Contre-mesure électronique consistant à entrer dans un réseau radioélectrique ennemi en se faisant passer pour l'un des membres de celui-ci. <p>Synonymes : immixtion, ingérence, intervention</p>	Larousse ²³
Intrusion	<p>a) Action de s'introduire illégalement dans une charge, une fonction, une dignité. (Dict. XIX^e et XX^e s.)</p> <p>b) Action de s'introduire dans un lieu, une société sans invitation, sans droit, sans y être attendu.</p> <p><i>Au fig.</i></p> <p>a) Action d'intervenir, de s'ingérer dans un domaine sans en avoir le droit.</p>	Cnrtl

3.1.2. Interception légale

Lawful interception	"Lawful interception's main task is to silently obtain network communications, giving access to intercepted traffic to lawful authorities for the purpose of data analysis and/or evidence. Such data generally consist of signaling, network management information, or in fewer instances, the content of network communications. If data cannot be obtained in real-time, the activity is referred to as access to retained data (data retention)" ²⁴ .
---------------------	---

« Les interceptions légales désignent les **interceptions judiciaires et les interceptions administratives** :

Dans le droit Français, la mise en place d'une interception est encadrée. Celle-ci peut être motivée dans le cadre d'une instruction judiciaire. Dans un tel contexte c'est le juge d'instruction qui requiert l'opérateur ; ce sont les écoutes judiciaires.

D'un autre côté, les écoutes administratives peuvent être demandées pour des raisons de défense nationale, de protection des intérêts de l'état, de lutte contre le terrorisme. Dans le cas de l'état Français, ce type d'interception est demandé par le premier ministre. »²⁵

Les systèmes d'interception légale sont, comme leur nom l'indique, des « systèmes », c'est-à-dire un ensemble de technologies, logiciels, équipements, dont le déploiement peut être variable en fonction des objectifs, des cibles, des besoins, des données recherchées, du lieu de l'interception (conditions, environnement), etc.

Les systèmes mis en place ont pour fonction de collecter deux catégories d'information :

²³ <http://www.larousse.fr/dictionnaires/francais/intrusion/44028?q=intrusion#43954>

²⁴ <http://www.release14.org/product-view/lawful-interception/>

²⁵ <http://www.orange-business.com/fr/blogs/securite/lois-reglementations-standards-et-certifications/interceptions-legales-retour-aux-bases>

- soit celles qui répondent à la question « qui » (informations de signalisation) : « Quels sont les numéros appelés, les appels ayant aboutis et ceux n'ayant pas débouché sur une conversation. »
- soit celles qui répondent à la question « quoi » (le contenu des communications) : « une conversation entre deux personnes, le contenu de mails, d'une session de messagerie instantanée ou encore des fichiers »²⁶

3.1.3. Interception stratégique, interception tactique

L'interception **tactique** désigne l'interception ciblée. L'interception **stratégique** désigne l'interception de masse. Si on s'en réfère à la distinction établie en 2013 sur le document ci-dessous, extrait de présentations de l'entreprise Ability²⁷, les distinctions entre les deux formes d'interception se font également sur le plan technique : avec l'interception de masse, c'est-à-dire ici en grandes quantités de données, de flux, il n'est pas possible de procéder au déchiffrement. L'interception ciblée permet de l'envisager.

Il faut distinguer l'interception pour gérer le système d'un point de vue technique de l'interception pour renseignement. *"T/A was used to assist intercept operators by providing current data on radio frequencies, callsigns, and transmission schedules used by the targets. In return, the intercept operators assisted the traffic analyst by their recognition of unique identifying characteristics of the target radio operators and their equipment, somewhat similar to recognizing the voice of a telephone caller. A significant challenge was maintaining a current database on all prospective targets. Having current technical data available allowed the intercept operator to access the desired communications without first spending weeks or months building background information on the target communications. Given the changing nature of communications, the building and maintaining of technical data were an important and never-ending process."*²⁸

L'interception est l'une des premières applications de l'analyse de trafic (T/A): *"The elementary function of traffic analysis in intercept control is the providing of basic net data to the stations. This includes chiefly frequencies, calls, schedules, and station locations."*²⁹

²⁶ Jean-François Audenard, Interceptions légales, retour aux bases, 2 novembre 2010, Blog Sécurité, <http://www.orange-business.com/fr/blogs/secureite/lois-reglementations-standards-et-certifications/interceptions-legales-retour-aux-bases>

²⁷ L'entreprise Ability est une société qui se présente comme un leader de l'interception tactique, qui propose des solutions d'interception, de géolocalisation, fournit les polices, les renseignements, les armées). https://www.sec.gov/Archives/edgar/data/1588869/000121390015008642/f8k092915a2ex99i_cambridge.htm

²⁸ Donald A. Borrmann, William T. Kvetkas, Charles V. Brown, Michael J. Flatley, and Robert Hunt, The History of Traffic Analysis: World War I – Vietnam, Center for Cryptologic History, National Security Agency, 2013, 60 pages, <https://cryptome.org/2013/07/nsa-traffic-analysis.pdf>

²⁹ Fundamentals of traffic analysis (radio – télégraph), Department of the Army and the Air Force, 1948, 108 pages, <https://cryptome.org/2015/04/nsa-traffic-analysis-1948.pdf>

Market Shift to Tactical Interception Plays to Ability's Strengths

Strategic Interception	Tactical Interception
» Mass interception of large networks (AT&T, T-Mobile)	» Targeted interception
» Network cooperation dependent	» Network cooperation not required
» Impossible to break encryption of IT traffic (data)	» Possible to break encryption
» Susceptible to leaks	» More confidential
» Declining budgets	» Growing budgets

↓

Ability is a leader in this emerging market

15

CAMBRIDGE
CAPITAL

Source : https://www.sec.gov/Archives/edgar/data/1588869/000121390015008642/image_015.jpg

3.1.4. Interception ciblée (targeted) et interception massive (bulk)

- « **Traffic** » désigne les communications transitant entre un émetteur/envoyeur et un récepteur³⁰
- « **Analyse de trafic** » (traffic analysis) désigne l'étude du trafic par un récepteur tiers (« unintended recipient »). En anglais on utilise l'acronyme T/A pour Traffic Analysis³¹. L'analyse de trafic désigne l'étude des caractéristiques externes (ie pas les contenus des messages) des communications ciblées. La T/A constituait une aide à l'entreprise des cryptanalistes (aide au déchiffrement)

La **distinction** entre **interception ciblée et massive** s'exprime de diverses manières :

- elle distingue les interceptions qui concernent **des cibles connues (interception ciblée)**, de celles (**massives**) **pratiquées lorsque les cibles ne sont pas connues**.
- **l'interception massive**, en masse, désigne la collecte de quantités massives de flux de données de l'internet mondial
- la **collecte massive** sert à découvrir (utilisée pour l'espionnage international, pour identifier des groupes, réseaux, individus constituant des menaces à a sécurité et défense nationale), quand la collecte ciblée est utile à l'enquête (elle vise des suspects notamment).

³⁰ Donald A. Borrmann, William T. Kvetkas, Charles V. Brown, Michael J. Flatley, and Robert Hunt, The History of Traffic Analysis: World War I – Vietnam, Center for Cryptologic History, National Security Agency, 2013, 60 pages, <https://cryptome.org/2013/07/nsa-traffic-analysis.pdf>

³¹ Ibid.

- « **ciblage** » s'applique aux individus (des personnes identifiées, particulières), mais aussi « lieu » (un quartier, une maison, etc.) Dans ce dernier cas, l'unité de lieu, définie par les besoins de l'enquête, ne signifie pas ciblage des personnes. Ainsi le recours à l'IMSI Catcher ne permet-il pas de discriminer, et d'assurer la seule interception des communications des personnes considérées comme suspectes ou faisant l'objet d'une surveillance policière.
- le terme de langue anglaise « bulk » désigne les interceptions « en vrac » ou « en masse », « massives ». Les interceptions « massives » sont également traduites en anglais par l'expression « massive interception ».

Targeted Intercetion (interception ciblée)	« this form of interception is used on UK citizens who are suspected of illegal activity; It can be conducted on a specific person or a specific location by the police, the intelligence agencies or the armed forces; The request must be specific as to who or what will be spied on and where; Targeted can also be used in a thematic way. Thematic means groups of people, an area of locations, a number of organisations » ³² .	2016
	« States have access to a number of different techniques and technologies to conduct communications surveillance of a targeted individual's private communications. Real-time interception capabilities allow States to listen to and record the phone calls of any individual using a fixed line or mobile telephone, through the use of interception capabilities for State surveillance that all communications networks are required to build into their systems. An individual's location can be ascertained, and their text messages read and recorded. By placing a tap on an Internet cable relating to a certain location or person, State authorities can also monitor an individual's online activity, including the websites he or she visits.» ³³	2013

Bulk Interception	"Bulk interception is a vital tool designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK" ³⁴	2015
Bulk Interception (interception en masse)	« Is done by tapping internet cables carrying the world's internet traffic; The intelligence agencies now have the lawful power to tap these cables and grab chunks of internet activity; Bulk interception if broad, rarely based on a specific investigation and is used to look for plots, behaviour or activity which may potentially be of a criminal or terrorist nature" ³⁵ .	2016
Bulk and targeted interception	"Interception is the ability to listen in on what someone says or writes. There are two types of interception in the Investigatory Powers Act; targeted and bulk. Targeted is used when the focus of the investigation is known. Bulk is used when the focus is unknown. Bulk interception describes the gathering of large chunks of internet traffic from around the world. Because bulk is used to discover rather than investigate it could be described as a form of pre-crime investigation" ³⁶ .	2016

³² <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Interception.pdf>

³³ Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Nations Unies, Assemblée Générale, 17 avril 2013, 23 pages, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

³⁴ Factsheet Bulk Interception, Investigatory Powers Bill, UK, 30 octobre 2015, 2 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk-Interception.pdf

³⁵ <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Interception.pdf>

³⁶ <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Interception.pdf> Site consulté le 1^{er} mars 2017

3.1.5. Interception passive, interception active

L'interception passive désigne le recours à des équipements qui ne font que recevoir et ne peuvent pas émettre, les rendant ainsi indétectables par la cible³⁷. Ces équipements sont utilisés pour intercepter les signaux radio entre un téléphone mobile et un émetteur, ou entre l'émetteur et d'autres éléments composant le réseau. Des solutions technologiques permettent de protéger les communications contre ce type d'interception³⁸. Le chiffrement des données émises entre le poste mobile et la borne sont prévues par la norme GSM et les suivantes.

Interception active et passive peuvent être utilisées pour surveiller les accès à Internet: « Dans le cas de l'interception active, les nœuds de réseaux disponibles, comme les routeurs et serveurs AAA, permettent de filtrer les données d'accès et les contenus de communication de la personne à surveiller. La méthode passive consiste quant à elle à placer des sondes réseau non intrusives qui sont intégrées au réseau de l'opérateur pour surveiller l'ensemble du trafic. Dans certains cas, la combinaison de la méthode passive et de la méthode active se révèle être la solution la plus appropriée».³⁹

3.2. La surveillance

La surveillance des communications ne se réduit pas à l'interception. Elle désigne un ensemble plus large de pratiques et donc de technologies : monitoring⁴⁰, interception, collecte, stockage, rétention d'information. Telle est par exemple l'approche que propose le site privacyinternational.org⁴¹ : « *Communications surveillance is the **monitoring, interception, collection, preservation and retention** of information that has been communicated, relayed or generated over communications networks to a group of recipients by a third party. [...] In turn, **communications surveillance is no longer limited to intercepting** a messenger or attaching a 'crocodile clip' to a telephone line. There are now four main methods of communications surveillance: internet monitoring, mobile phone interception, fixed line interception, and intrusion technologies (which are explained in detail below). Surveillance over internet, mobile, and fixed-line networks can take place with or without the cooperation of the network operator ...* »⁴²

Retenons ici de la « surveillance » les définitions du Larousse et du CNRTL.

<ul style="list-style-type: none">- Observer attentivement quelqu'un, quelque chose pour les contrôler- Observer un lieu, regarder avec attention ce qui s'y passe- Veiller sur quelqu'un, quelque chose dont on a la garde, la responsabilité <p>Synonymes : Observer attentivement quelqu'un, quelque chose pour les contrôler</p>	Larousse ⁴³
--	------------------------

³⁷ <http://www.cryptophone.de/en/background/gsm-insecurity/passive-gsm-interception/>

³⁸ <http://www.cryptophone.de/en/background/gsm-insecurity/passive-gsm-interception/>

³⁹ <https://lirms.utimaco.com/fr/solutions/solution-lawful-interception-management/solutions-destinees-aux-operateurs-de-reseaux-fixes/>

⁴⁰ Le monitoring est juste le suivi de la densité de l'activité ; les outils de monitoring peuvent être détournés pour faire de l'interception ; l'interception est un but

⁴¹ PrivacyInternational est une ONG internationale qui œuvre à la défense des droits fondamentaux, pour la protection de la vie privée et en dénonce les atteintes commises par les gouvernements et les organisations. Elle a été créée en 1990, est basée à Londres, dispose d'un bureau à Washington. Ses investigations portent sur les pratiques de surveillance. Elle unit ses efforts à ceux d'autres ONG, telle que l'EPIC (Electronic Privacy International Center) aux Etats-Unis. PrivacyInternational publie des études classant les pays en fonction de leur attachement au respect de la vie privée.

⁴² <https://www.privacyinternational.org/node/10>

⁴³ <http://www.larousse.fr/dictionnaires/francais/surveiller/75899?q=surveiller#75030>

Action ou fait de surveiller une personne dont on a la responsabilité ou à laquelle on s'intéresse.	CNRTL ⁴⁴
Activité policière consistant à surveiller des personnes suspectes ou des milieux à risques, pour prévenir des actions délictueuses ou criminelles, pour garantir la sécurité publique.	
Action de surveiller un lieu et ses environs pour se prémunir contre une agression.	

In fine l'interception a pour finalité la surveillance.

3.3. Les données

L'Assemblée générale des Nations Unies, dans un rapport de 2013 portant sur la liberté d'opinion et d'expression, s'interroge sur le large spectre de catégories de données exposées aux pratiques de la surveillance : *"The dynamic nature of technology has not only changed how surveillance can be carried out, but also "what" can be monitored. In enabling the creation of various opportunities for communication and information-sharing, the Internet has also facilitated the development of large amounts of transactional data by and about individuals. This information, known as communications data or metadata, includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive. Communications data are storable, accessible and searchable, and their disclosure to and use by State authorities are largely unregulated. Analysis of this data can be both highly revelatory and invasive, particularly when data is combined and aggregated. As such, States are increasingly drawing on communications data to support law enforcement or national security investigations. States are also compelling the preservation and retention of communication data to enable them to conduct historical surveillance"*.⁴⁵

Nous distinguons ci-après les catégories de données suivantes, que nous retrouvons de manière constante dans les discours traitant de la surveillance et de l'interception des communications électroniques : tout d'abord le signal physique, puis la donnée brute, les données interprétées et les métadonnées.

3.3.1. Le signal physique

Le **signal physique** est le résultat brut de l'interception. Dans le cas du téléphone filaire, il s'agit du signal électrique issu directement de la ligne. Pour les données numériques, il s'agit des données brutes (*raw data*), sous la forme d'une suite binaire de symboles 0 et 1.

La transformation de ce signal en information utile nécessite la connaissance de la modulation, codage du canal, et du codage de source.

La modulation décrit le procédé pour transformer un signal porteur d'information, comme celui issu d'un microphone par exemple, en un signal transmissible sur le vecteur considéré, comme une onde électromagnétique par exemple.

Dans le cas d'information analogique, la modulation de fréquence ou d'amplitude est utilisée sur les canaux de diffusion de radio ou de télévision analogique.

⁴⁴ <http://www.cnrtl.fr/definition/surveillance>

⁴⁵ http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Les **signaux numériques** sont souvent modulé par une modulation de phase qui associe une phase plus ou moins 90 degrés à un symbole 0 ou un 1.

3.3.2. La donnée brute

Les **données brutes** en elles-mêmes ne portent pas directement d'information. L'extraction d'informations utiles à partir des données brutes nécessite la connaissance des traitements qui conduisent jusqu'au signal transmis. Ces traitements ne sont pas souvent secrets et obéissent à des standards. Parfois, un traitement propriétaire gêne le travail de l'intercepteur.

3.3.3. Les données interprétées

Les **données interprétées** sont celles qui portent l'information qui intéresse l'intercepteur. Il peut s'agir de la transcription d'une conversation, d'image (fax, photos), de vidéo, de texte, voire de code binaire d'un programme exécutable. Une fois le signal démodulé et les erreurs corrigées, il peut subsister un chiffrement destiné à empêcher à quiconque n'est pas dans le secret d'une convention établie entre les correspondants d'accéder aux informations utiles (voir plus loin le paragraphe sur la cryptographie).

Lors de sa propagation sur le câble ou par voie radio, le signal subit une altération physique fortuite due au bruit, aux parasites, aux perturbations électromagnétiques, aux interférences, au brouillage, à l'affaiblissement du aux conditions de propagation, etc. L'information portée par le signal peut alors ne pas être transférée correctement à destination. Pour se prémunir de ce défaut, les données numériques subissent un traitement qui consiste à ajouter une redondance qui permettra de corriger automatiquement les erreurs. Les codes les plus fréquents sont les codes BCH, du nom de leurs inventeurs Bose, Ray-Chaudhuri et Hocquenghem, et les codes de Reed-Solomon.

3.3.4. Les métadonnées

Métadonnée	Donnée servant à caractériser une autre donnée, physique ou numérique : Les métadonnées sont à la base de l'archivage.	Larousse ⁴⁶
------------	--	------------------------

Les données de communication (métadonnées) sont également définies ainsi: *“Communications data: information about an individual’s communications (e-mails, phone calls and text messages sent and received, social networking messages and posts), identity, network accounts, addresses, websites visited, books and other materials read, watched or listened to, searches conducted, resources used, interactions (origins and destinations of communications, people interacted with, friends, family, acquaintances), and times and locations of an individual, including proximity to others)”*⁴⁷.

Le terme « **métadonnées** » désigne toute information extraite du signal qui ne concerne pas directement l'information échangée :

- Qui communique avec qui ? Qui est l'expéditeur ? Qui est le destinataire ?
- Quelle est la taille des données échangées : un bref appel de quelques secondes ? Ou une conversation de plusieurs heures ?

⁴⁶

<http://www.larousse.fr/dictionnaires/francais/m%C3%A9tadonn%C3%A9e/186919?q=m%C3%A9tadonn%C3%A9e#10928381>

⁴⁷ http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

- Quelle est la nature des données échangées : texte ? Image ? Son ? Code ? Télécommande d'un équipement ?
- où se trouve l'émetteur et le destinataire ? (géolocalisation)
- Quelle est la fréquence des échanges ?

Dans les communications TCP/IP, des métadonnées sont associées à chaque paquet : source et destination IP, numéro de port TCP par exemple (le port indique la nature de l'échange : le port 25 correspond à l'utilisation de l'e-mail).

Des métadonnées sont également associées aux appels passés par téléphone mobile (appelant, appelé, géolocalisation, durée de la communication...)⁴⁸ L'étude des métadonnées va ainsi fournir des indications sur l'existence et la nature des relations, l'existence et configuration de réseaux, etc. Les informations, indicateurs, émanent des changements de pratiques des utilisateurs (se mettre à crypter ses échanges indique une modification dans la nature des échanges...)

L'exploitation des métadonnées se heurte toutefois à des contre-mesures : les messageries sécurisées masquent les métadonnées l'utilisation d'outils qui comme Tor masquent les métadonnées.

Alors que la réglementation protège le caractère privé des informations échangées, les métadonnées sont librement accessibles et ne sont pas considérées comme privées. Le Règlement Général sur les données personnelles de l'UE prévoit "une protection des données à caractère personnel" sans pour autant protéger explicitement les métadonnées, la protection semble se limiter à une anonymisation lorsque les données peuvent être associées à une personne⁴⁹.

Les services de renseignement affirment⁵⁰ que ces métadonnées constituent un bagage suffisant dans la plupart des cas pour cartographier des réseaux mafieux ou terroristes, pour avoir une idée assez précise sur leur activité.

Une brusque recrudescence de l'activité d'un groupe de correspondants surveillés peut ainsi être interprétée comme le signal d'une opération en cours de préparation.

L'argument selon lequel la collecte des métadonnées poserait moins de problèmes (en termes de respect de la législation sur les données et la vie privée) contrairement à l'analyse des contenus des communications électroniques, est discutable (voir le rapport européen cité en note de base de page)⁵¹ : en effet, ces données ne sont pas strictement techniques. Elles sont, pour nombre d'entre elles, des données à caractère personnel (un numéro de téléphone, une adresse IP, ...) et définies comme telles par le droit.

⁴⁸ John McDermott, What are traffic analysis and metadata?, 3 février 2016, <http://blog.learningtree.com/what-are-traffic-analysis-and-metadata/>

⁴⁹ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

⁵⁰ - <http://www.aiservice.fr/News/2013/Decembre/depannage-informatique-domicile-paris-0173-metadonnees-et-renseignement-une-nouvelle-ere-de-lespionnage-lutilisation-des-algorithmes.html>
- http://lexpansion.lexpress.fr/high-tech/loi-sur-le-renseignement-tout-ce-que-les-metadonnees-peuvent-dire-de-vous_1677322.html

⁵¹ Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Article 29 Data Protection Working Party, 819/14/EN, Adopted on 10 April 2014, 16 pages, Bruxelles, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

"In Europe metadata are personal data and should be protected ⁵²:

- *Article 2(a) Directive 95/46/EC, personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly".*
- *définition reprise dans l'article 2(a) of Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data"*

Les métadonnées révèlent parfois plus d'informations que les contenus eux-mêmes. Il y a donc potentiellement atteinte à la vie privée (analyse des habitudes des individus des relations entre individus, etc.)

Nul besoin de lire les correspondances pour « profiler » et tracer les cybernautes. « 10 % de données produisent 90 % de métadonnées [...] A partir d'une information émise, les algorithmes peuvent facilement récupérer les dates de connexion, les sites consultés et la fréquence des consultations. Facebook, « la meilleure agence de renseignement au monde », ne procède pas autrement ».

IV - Méthodes, techniques et technologies de cybersurveillance/interception

Les communications entre ordinateurs distants par le réseau Internet obéissent à un protocole de transmission organisé en plusieurs couches. Les quatre couches standards du réseau Internet sont :

- Application
- Couche transport TCP (*Transport Control Protocol*)
- Couche Internet IP (*Internet Protocol*).
- Accès au réseau.

L'application interagit avec l'utilisateur de l'ordinateur. Elles ont pour nom http (*HyperText Transfert Protocol*), pop (*Post Office Protocol*), smtp (*Simple Mail Transfert Protocol*), etc.

A l'autre extrémité, se trouve la couche d'accès au réseau chargé de la transformation des données en signal physique : signal électrique dans le cas d'une transmission ADSL sur une ligne téléphonique, ou radio-électrique dans le cas d'une transmission sans fil de type Wifi.

Entre les deux on trouve les couches TCP et IP caractéristiques du réseau Internet.

L'application dialogue avec la couche transport chargée de tous les mécanismes nécessaires à un transfert fiable des données. Elle assure la fragmentation et le ré-assemblage des données en paquets, la réinsertion dans l'ordre des paquets manquants, de la détection et de la correction des erreurs.

La couche Inter réseaux (Internet) a été définie de manière à pouvoir connecter de nombreux réseaux entre eux. Cette couche traite chaque paquet indépendamment des autres. Sa fonction principale est l'acheminement correct du paquet au destinataire. Cela repose sur la notion d'adresse, qui est une donnée, à l'origine de 32 symboles binaires (IPv4), portée aujourd'hui à 128 symboles binaires (IPv6) et qui identifie la machine destinatrice du paquet. Une partie de l'adresse identifie le réseau, et l'autre partie identifie la machine dans le réseau. Une adresse de 32 symboles binaires ne peut adresser qu'un peu plus de 4 milliards de destinations (moins d'un habitant de la planète) alors qu'une adresse de 128 symboles binaires peut en théorie adresser toutes les bactéries présentes sur terre (estimées à 10^{30} , alors que 2^{128} vaut environ 3×10^{38}).

⁵² Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Article 29 Data Protection Working Party, 819/14/EN, Adopted on 10 April 2014, 16 pages, Bruxelles, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

Les données utiles (voix, image, texte) issues de l'application peuvent subir un traitement comme le chiffrement ou la compression. Elles sont alors encapsulées dans un nouveau paquet dont l'entête indique le traitement effectué.

L'accès aux données utiles nécessite alors une analyse en profondeur des paquets (DPI *Deep Packet Inspection*), ce qui ralentit considérablement le traitement effectué par l'interception, voire l'interdit dans le cas d'un chiffrement des données.

Il existerait essentiellement deux méthodes d'interception du trafic IP ⁵³ :

- l'interception du trafic dans le réseau IP du fournisseur internet (méthode dite passive) : dans ce cas le filtrage du trafic IP est intégré au système d'interception qui reçoit toutes les données brutes, qui doivent ensuite être filtrées, traitées, décodées, lues. La limite de cette approche réside dans le fait que les flux VPN, https, Skype, PGP, sont chiffrés et ne peuvent pas toujours être simplement décryptés.
- en essayant d'obtenir un accès direct à l'ordinateur cible, via des outils d'intrusion (malwares). Cette méthode permet de palier les limitations de la méthode précédente, car en amont du processus de crypto des données. Cette méthode permet une interception ciblée.

4.1. Pour une typologie des technologies d'interception et de cybersurveillance

La cybersurveillance et l'interception de communications électroniques comme nous l'avons rappelé dans le chapitre précédent, désignent plusieurs catégories d'action, et supposent donc des techniques adaptées à l'objectif, des technologies spécifiques. L'interception ne s'arrête pas à la capture du message, des données, du signal. Il faut adjoindre des systèmes de stockage, de traitement, d'analyse. L'interception qui veut capter un message pour en prendre connaissance, ne recourt pas aux mêmes moyens que celle qui vise à arrêter les messages.

L'ensemble des technologies, techniques, capacités techniques d'interception et cybersurveillance est donc a priori extrêmement large. Il convient de tenter de les regrouper afin d'avoir une vision schématisée, simplifiée des grandes catégories de techniques et technologies qui peuvent être impliquées et mobilisées. La littérature existante nous offre quelques pistes.

Le site privacyinternational.org identifie 4 catégories de technologies pouvant être mobilisées pour la surveillance des communications :

- 1 la surveillance d'internet (internet monitoring),**
- 2 le monitoring de la téléphonie mobile,**
- 3 l'interception de la téléphonie fixe,**
- 4 les technologies d'intrusion.**

La notion d'interception est ici réservée aux opérations portant sur la téléphonie fixe. Pour internet et la téléphonie mobile, le site mobilise plutôt la notion de « monitoring ». L'intrusion désigne un ensemble de pratiques agressives de surveillance.

La notion de « cybersurveillance » n'est par ailleurs pas utilisée, les auteurs préférant celle de « surveillance des communications ».

⁵³ <http://aqt-technology.com/ip-interceptions-web-email-skype> (site consulté le 1^{er} février 2017)

- le monitoring d'internet consiste ici en la capture des données. Les technologies peuvent être déployées en n'importe quel point des systèmes physiques et électroniques de l'internet (les câbles, les serveurs, les routeurs, les fournisseurs, etc.) Il est possible d'utiliser des outils techniques (pour se connecter physiquement aux réseaux) et logiciels (le monitoring n'est pas uniquement interception : l'analyse des données de l'internet relève de ce monitoring)
- le monitoring de la téléphonie mobile consiste en la capture de l'information (ie les données). L'une des technologies phares de cette surveillance est l'IMSI Catcher. Cet outil permet d'intercepter, au sens « capter », mais également d'envoyer des messages aux téléphones. Il ne s'agit donc pas d'interception passive, mais bien de s'immiscer dans le réseau et les échanges.
- l'interception des communications fixes (« fixed line interception ») concerne la capture de l'information qui circule sur les réseaux de téléphonie fixe (public switched telephony networks – PSTN) Les solutions technologiques vendues par les entreprises permettent aujourd'hui de surveiller des réseaux de ce type à l'échelle d'un pays tout entier.

L'intrusion permet de déployer clandestinement des malwares sur les téléphones mobiles et les ordinateurs, permettant aux opérateurs de prendre la main sur les appareils cibles. Le site Privacy International affirme que l'intrusion est certainement l'une des formes de surveillance les plus invasives qui soit.

La Commission Européenne dans sa définition du périmètre des technologies duales et de la réglementation afférente (reformulation en date du 28 septembre 2016 des règles en matière d'exportation de technologies duales, visant à empêcher que des technologies qui ont un usage légitime dans le cadre des interceptions légales, ne soient fournies à des régimes autoritaires, ou ne permettent de porter atteintes aux droits de l'homme)⁵⁴, intègre les technologies de cybersurveillance. Dans ce document de septembre 2016⁵⁵, la Commission propose de modifier la définition des technologies duales, pour intégrer les particularités de nouvelles technologies, dont celles de cybersurveillance, ce qui n'était pas le cas jusqu'alors selon l'arrangement de Wassenaar...

« Les «technologies de cybersurveillance» sont des biens spécifiquement conçus pour permettre l'intrusion secrète dans des systèmes d'information et de télécommunication afin de surveiller, d'extraire, de collecter et d'analyser des données et/ou de paralyser ou d'endommager le système visé, y compris les biens qui se rapportent aux technologies et équipements ci-après:

- a) les équipements d'interception de télécommunications mobiles;**
- b) les logiciels d'intrusion;**
- c) les centres de surveillance;**
- d) les systèmes d'interception licite et de conservation de données;**
- e) l'investigation numérique »⁵⁶**

⁵⁴ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast), Brussels, 28.9.2016, COM(2016) 616 final , 2016/0295 (COD) , 45 pages, http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf Texte en français: <https://ec.europa.eu/transparency/regdoc/rep/1/2016/FR/1-2016-616-FR-F1-1.PDF>

⁵⁵ qui vient concrétiser des intentions affichées dès 2011, notamment suite aux révélations de WikiLeaks concernant les activités d'Amesys en Libye

⁵⁶ <https://ec.europa.eu/transparency/regdoc/rep/1/2016/FR/1-2016-616-FR-F1-1.PDF>

La proposition initiale de la refonte des réglementations prévoyait un ensemble plus large de catégories :

- Mobile telecommunications interception equipment;
- Intrusion software;
- Monitoring centres;
- Lawful Interception (LI) systems and data retention systems;
- Biometrics;
- Digital forensics;
- Location tracking devices;
- Probes;
- Deep Packet Inspection (DPI) systems⁵⁷

Ont ainsi notamment été écartés:

- les équipements biométriques,
- les dispositifs de localisation
- les systèmes d'inspection de paquets en profondeur⁵⁸.

Le SIPRI rappelle que les technologies de filtrage et blocage d'internet sont largement utilisées pour d'autres applications ou objectifs que la censure⁵⁹.

Toujours selon une étude du SIPRI (novembre 2015), ces technologies doivent être analysées au regard de contraintes multiples⁶⁰: *“The different cyber-surveillance technologies identified by the study vary significantly in a number of areas, including: (a) the extent to which they have non-surveillance applications; (b) whether or not they are currently affected by EU dual-use export controls, (c) the range of security and human rights concerns attached to their export and use; (d) how extensively they are used by EU Member State law enforcement agencies (LEAs) and intelligence agencies; (e) whether or not there are agreed standards relating to their use; and (f) the number and type of EU and non-EU based companies that are engaged in their production”*⁶¹.

4.2. Techniques, technologies, méthodes et dispositifs d'interception

4.2.1. Différentes méthodes d'interception

4.2.1.1. Interception à la source

Le principe est de placer des micros dans les locaux où ont lieu les conversations à surveiller, à l'instar de l'affaire des *Plombiers du Canard Enchaîné*, où deux « plombiers », qui sont en réalité des agents de la DST, sont surpris, le 3 décembre 1973, en train de placer des mouchards dans les nouveaux bureaux de l'hebdomadaire satirique.

⁵⁷ Deep Packet Inspection (DPI) systems; “used to examine the content of data as it passes through a communications network”; “DPI systems are also employed when a state bypasses standardized Lawful Interception processes through the use of a ‘tap’ or a ‘black box’” (“probes and DPI systems are also used in a range of non-surveillance technologies and systems”)

⁵⁸ <http://www.silicon.fr/europe-recadrer-exportation-technologies-cybersurveillance-159245.html>

⁵⁹ <https://www.sipri.org/sites/default/files/final-report-eu-dualuse-review.pdf>

⁶⁰ “Data and information collection for EU dual-use export control policy review”, rapport du SIPRI, 6 novembre 2015, 247 pages, <https://www.sipri.org/sites/default/files/final-report-eu-dualuse-review.pdf>. Rapport page 15

⁶¹ Pour une description des technologies, reprendre le rapport Sipri page 154 et suiv. <https://www.sipri.org/sites/default/files/final-report-eu-dualuse-review.pdf>

Un procès a eu lieu, et, malgré les nombreuses preuves apportées par le journal, les services de renseignement ont toujours nié être à l'origine de ces actions, conduisant à une ordonnance de non-lieu rendue le 29 décembre 1976, précisant qu'au moment des faits, les locaux étaient toujours inoccupés, et qu'il ne pouvait y avoir ni violation de domicile, ni atteinte à la vie privée.

Des affaires similaires ont été mises en évidence dans les locaux d'ambassades occidentales à Moscou durant la guerre froide.

Ce procédé d'interception à la source par des mouchards est :

- difficile à mettre en œuvre,
- le plus souvent opéré par les services de renseignement
- risqué et le plus souvent illégal.

4.2.1.2. Interception pendant la transmission

La correspondance peut être interceptée pendant sa transmission, à l'instar de l'ouverture du courrier par les cabinets noirs. L'ouverture du courrier nécessite des efforts pour rester discrets. L'occupant allemand a résolu le problème en mettant en place les « cartes postales interzone » à partir de 1941, le dispensant de procéder à de nombreuses et coûteuses ouvertures de courrier.

Après avoir complété cette carte strictement réservée à la correspondance d'ordre familial, biffer les indications inutiles. — Ne rien écrire en dehors des lignes.
ATTENTION. — Toute carte dont le libellé ne sera pas uniquement d'ordre familial ne sera pas acheminée et sera probablement détruite.

La Chaux, le 14 Décembre 1940

Je suis en bonne santé fatigué
légèrement, gravement malade, blessé.
~~libre~~ prisonnier.
décédé sans nouvelles.
La famille va bien.
~~Desen de provisions~~ d'argent.
nouvelles, bagages. est de retour à
travaille à
à l'écrit de a été reçu
à
le
avez reçu ma lettre recommandée du 10 juin contenant le
reçu de ma retraite échu le 2 Avril 1940
Affectueuses pensées. Baisers.
Signature.
Leprieux

4.2.1.3. Les interceptions téléphoniques

Une méthode consiste en la pose de prises de cuivre sur les câbles du réseau téléphonique par des services de police ou des officines privées⁶². L'inconvénient de cette pratique est sa difficulté de mise en œuvre, sa visibilité, et son illégalité⁶³.

⁶² http://lexinter.net/JF/interception_de_telecommunications.htm

Les écoutes légales nécessitent la coopération technique de l'opérateur.

4.2.1.4. Les interceptions radio

Les communications optiques ou radio électriques sont par nature sensible à l'interception. L'interception est dans ce cas facile, discrète et indétectable. Pour cette raison les communications radio nécessitent l'emploi d'un codage secret. Lorsque le télégraphe optique de Chappe a été mis en place, le codage était inconnu des employés qui se contentaient de reproduire le signal sans avoir connaissance de l'information véhiculée. L'organisation était très hiérarchisée et le codage n'était connu que des directeurs de station.

Dans le système de téléphonie mobile, les communications hertziennes sont chiffrées.

L'accès à l'information nécessite un travail de décryptement, et de disposer d'importantes équipes pour assurer ce travail, à l'instar de ce qu'ont mis en place les autorités polonaises avant la deuxième guerre mondiale pour accéder aux contenus des communications allemandes chiffrées par la machine *Enigma*, suivis par les britanniques de *Bletcheley Park*⁶⁴.

4.2.1.5. Les communications numériques

Cette classification des moyens d'interception reste pertinente pour les communications numériques actuelles sur Internet.

Le branchement d'une prise physique sur les câbles du réseau Internet reste une pratique efficace.

L'interception au niveau des routeurs, nécessite théoriquement la coopération des opérateurs. Les dispositions légales de certains pays obligent les opérateurs à coopérer avec les services de renseignement tout en étant empêchés de rendre publique cette coopération.

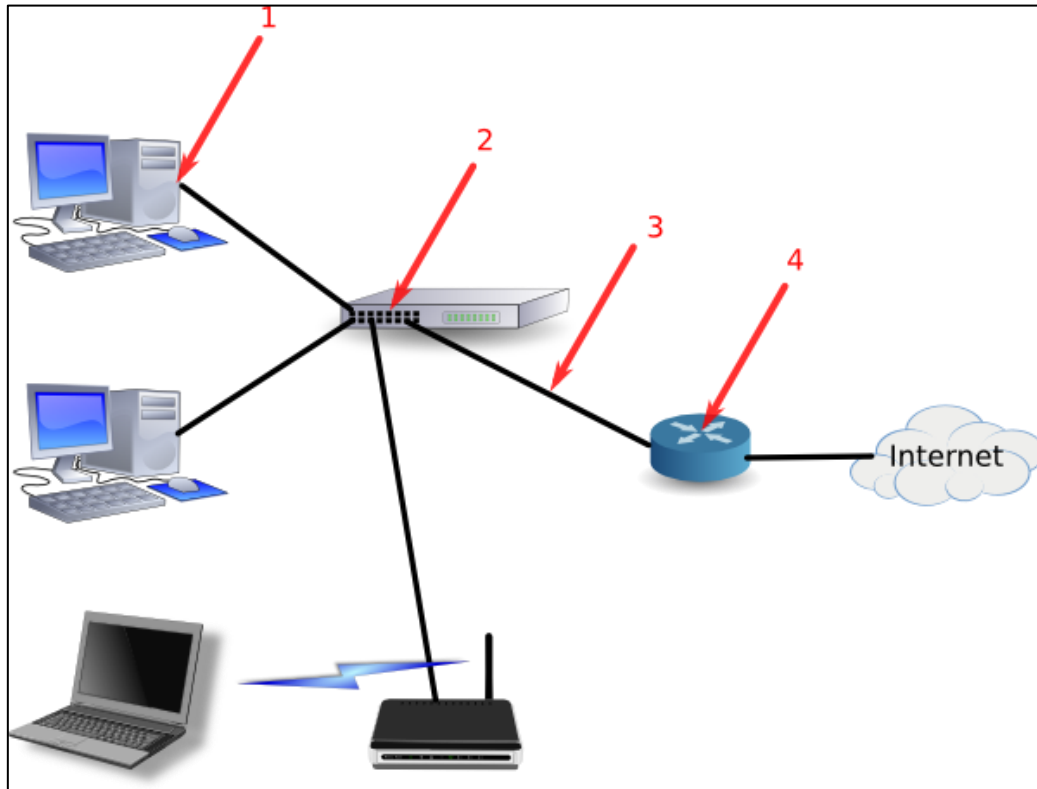
La complexité croissante des systèmes le rend vulnérables à des failles logicielles fortuites ou créées intentionnellement (*backdoors*).

De plus, la connectivité et la topologie du réseau autorise une grande souplesse géographique. Il n'y a pas d'obstacle technique pour qu'une station située à Paris puisse intercepter une communication entre Lyon et Marseille par action à distance sur le routage de la transmission.

⁶³ Huyghe F.B. (2009), *Les écoutes téléphoniques*, P.U.F., coll "Que sais-je ?"

⁶⁴ Cette activité a apporté un avantage notable aux forces alliées réduisant, selon les estimations, la durée du conflit de 6 mois à 2 ans.

4.2.1.6. L' « interception » pour la gestion des réseaux locaux



Source : <http://www.justasysadmin.net/files/3812/8406/4061/ReseauInterneIntercepSmall.png>

L' « interception de trafic » peut être nécessaire à la gestion d'un réseau local. Ces méthodes et technologies permettent⁶⁵ par exemple de diagnostiquer des problèmes réseaux entre machines ou d'optimiser la qualité de service. Il est possible dans l'exemple décrit dans le schéma ci-dessus, de mettre en place une « interception » à chacun des 4 points identifiés : au point 1 faire tourner un outil de capture de paquet (à l'aide d'outils de capture comme wireshark ou tcpdump) ; au point 2 faire du « port mirroring » (port miroir qui permet de faire ressortir, renvoyer, le trafic des autres ports) ; au point 3 faire un brigde (pont) qui consiste à placer une machine entre flux entrant et sortant, ce qui permet de modifier, manipuler les données, sélectionner les données sortantes, etc. ; enfin au point 4 , l'interception au niveau du routeur.

Un court article publié sur le site Justasysadmin.net précise qu'« il est à noter qu'accéder au paquet n'est pas suffisant pour accéder aux informations échangées, par exemple, dans le cadre d'une session https vers le site de votre banque, les paquets sont chiffrés et leur déchiffrement est très très long. De plus, lors d'établissement de session on peut vérifier l'identité du serveur que l'on cherche à joindre. Dans ce cas une redirection de trafic est très rapidement détectée par l'utilisateur »⁶⁶.

4.2.2. De l'analyse de trafic à l'exploitation des métadonnées

L'analyse de trafic, introduite par Gordon Welchman durant la seconde guerre mondiale, désigne l'interception et l'examen de messages en ne s'appuyant pas sur les contenus, qui peuvent donc être chiffrés sans que cela ne perturbe le processus, mais sur les données accompagnant le message : date, heure, origine, destinataire, etc.

⁶⁵ <http://www.justasysadmin.net/fr/theoretical/interception-de-traffic/>

⁶⁶ <http://www.justasysadmin.net/fr/theoretical/interception-de-traffic/>

Ces quelques données peuvent fournir des informations sur les intentions et actions des acteurs reliés au message. Il faut donc dans l'analyse de trafic procéder par déductions, recoupements, croisements, analyse de réseaux, etc. L'analyse de trafic s'appuie notamment sur des outils et méthodes d'analyse des réseaux sociaux.

- l'analyse de trafic puis le renseignement fondé sur l'exploitation des métadonnées ne traite pas les contenus des messages
- la cryptographie, qui s'applique aux contenus, ne fait donc pas obstacle à l'analyse de trafic et de métadonnées
- Plus le nombre de messages intercepté est élevé, plus le trafic révèle d'informations, plus la quantité de déductions, de croisements peuvent être réalisées et le nombre et qualité d'information révélés. L'analyse de trafic a donné naissance à l'analyse des métadonnées, qui nécessitent toutes deux l'interception massive et le stockage massif de données. Pendant la seconde guerre mondiale, les casseurs de code de Bletchley ont imaginé l'analyse de trafic pour contourner en partie les limites du déchiffrement. Les messages chiffrés par Enigma portaient en en-tête des informations ou données, un préambule comportant certains discriminants. De l'analyse de ces données, sans s'intéresser aux contenus, les équipes de Bletchley étaient parvenues à classer les messages en différentes catégories, en fonction de leur provenance notamment (pays, type de force, etc.) Ces informations, affinées, fournissaient alors des informations sur les déplacements des forces par exemple⁶⁷.

4.2.3. Intégrer les équipements d'interception à la source même des infrastructures/architectures de télécommunication

Dans de nombreux Etats, les fournisseurs de télécommunications ont été contraints d'adapter leurs infrastructures pour permettre une surveillance directe, se passant de l'autorisation des juges. Ce fut le cas en Colombie en 2012, en Ouganda en 2010 (où la loi de régulation des interceptions de communication⁶⁸ prévoit la création d'un centre de monitoring et ordonne que les fournisseurs de télécommunication transmettent les communications interceptées à ce centre)⁶⁹. Les autorités indiennes ont proposé qu'un système de monitoring centralisé redirige toutes les communications vers le gouvernement permettant ainsi aux agences de sécurité de se passer de toute demande aux fournisseurs mais aussi de toute autorisation du juge. La tendance est donc dans de nombreux pays à la séparation entre police et justice, pouvoir central et toute forme de contrôle ou restriction des juges, et au raccourcissement des procédures, et donc des délais. Les Etats veulent disposer d'une vision en temps réel, totale, sur les communications. L'option envisagée par l'Inde vise même à se passer de l'intervention des fournisseurs. Les risques sont bien sûr importants, en termes de transparence, de justice, car laissent la porte ouverte à toutes les dérives, tous les abus de pouvoir, à un état de surveillance, un Etat sans responsabilités.

La coopération des opérateurs de télécoms est-elle nécessaire ? Les cas de figure vont en fait dépendre des objectifs poursuivis et des conditions de réalisation des interceptions, ainsi que du type de données que les acteurs souhaitent intercepter, et des capacités de la technologie.

⁶⁷ F.H. Hinsley, A. Stripp, Codebreakers: the inside story of Bletchley Park, Oxford University Press; Reissue edition, August 2001, 360 pages

⁶⁸ Regulation of Interception of Communications Act 2010

⁶⁹ http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf


- «Tout opérateur de services de télécommunications est tenu de mettre en place les moyens nécessaires pour intercepter les communications échangées sur un réseau public. »⁷⁰
- « L'interception ne donne lieu à aucun enregistrement de la part de l'opérateur, ce qui lui est légalement interdit, mais uniquement à "l'aiguillage" de la communication" vers le service adéquat de l'état (en fait les flux transitent via la plateforme de médiation). Seule une personne dûment mandatée par le ministère de la justice ou les services du premier ministre peut effectuer l'écoute, le cadre de ce type d'actions étant strictement contrôlé par la loi. »⁷¹

ability

ULIN (Ultimate Interceptor) - Transformational Technology

- » New technology for interception of mobile devices
- » Unique to Ability - No known competitors
- » Cooperation of Network Operator (AT&T, T-Mobile) not required
- » Developed in house
- » Revenue model:
 - System
 - Software License
 - Maintenance & Support
- » High margin expansion
- » First orders expected 1Q 2016

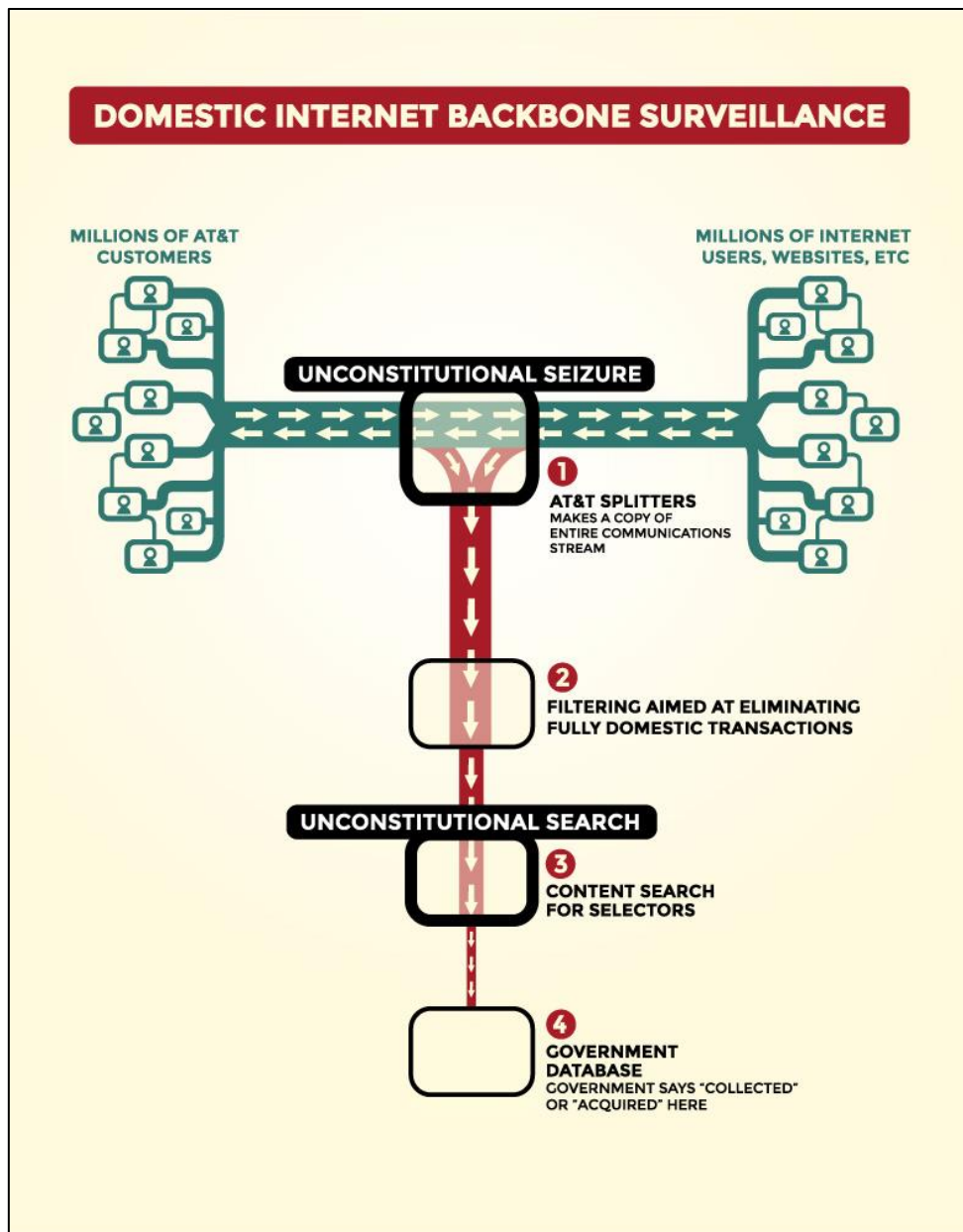
19



Source : https://www.sec.gov/Archives/edgar/data/1588869/000121390015008642/image_019.jpg

⁷⁰ <http://www.orange-business.com/fr/blogs/securite/lois-reglementations-standards-et-certifications/interceptions-legales-retour-aux-bases>

⁷¹ <http://www.orange-business.com/fr/blogs/securite/lois-reglementations-standards-et-certifications/interceptions-legales-retour-aux-bases>



Source : <https://www.eff.org/files/2014/07/24/backbone-3c-color.jpg>

Les compagnies de télécommunication ont laissé la NSA installer des équipements de surveillance (tel que le Narus Semantic Traffic Analyzer, instrument puissant de DPI)⁷² directement connectés aux réseaux, et installés dans des lieux protégés, dans les locaux mêmes des entreprises de télécommunication⁷³. Ces pratiques ont eu lieu en dehors de tout cadre légal (pas d'autorisation du juge, pas de discrimination entre données de citoyens américains et étrangers, etc.) Les données collectées font ensuite l'objet d'analyses, traitement (data mining). Ces équipements ont été installés suite aux attentats de septembre 2001. Rapidement les capacités d'interception puis de traitement ont augmenté. Une dizaine - peut-être le double – de ces équipements aurait été déployés chez les opérateurs américains au cours des années 2000. Au cours des ans, les volumes de données de

⁷² Selon les affirmations (2006) de l'Electronic Frontier Foundation, invoquant le rôle de l'opérateur AT&T dans la surveillance des communications de ses clients par la NSA.

⁷³ "How the NSA's domestic spying program works", <https://www.eff.org/nsa-spying/how-it-works>, site consulté le 1^{er} février 2017

communication n'ont cessé de croître, et parallèlement les capacités de collecte, les puissances de calcul et de traitement des données collectées, ainsi que les besoins de stockage (car les données ne sont pas effacées, du moins pas toutes). A l'expansion des masses de données produites par les utilisateurs/internautes/citoyens, répond une stratégie du « toujours plus » de la part des acteurs de la sécurité et de la défense qui n'envisagent pas d'autre option que l'expansion de leurs moyens et capacités, sur trois points clefs : la collecte (comment collecter davantage, mieux, plus vite), le traitement, l'analyse (de nouveaux calculateurs, de nouveaux algorithmes), le stockage (conserver autant de données que possible, susceptibles de servir ultérieurement, en étant croisées à de nouvelles données). L'immensité des capacités requises pouvait donc difficilement rester du domaine du secret. L'ambition qui consiste à s'assurer de la vision totale, la plus large possible, par le biais de l'exploitation des données électroniques, impose de repousser chaque jour davantage les limites des possibilités, car il faut pouvoir désormais collecter les données email, des sites, des réseaux sociaux, de tous les types d'application du net (deep et dark web, contenus chiffrés, etc.) et issus de la grande diversité de capteurs (internet des objets, parkings, véhicules, bornes, agendas électroniques, etc.) C'est dans l'optique d'un stockage massif que le data center de l'Utah⁷⁴ a été conçu.

L'Europe de son côté, avec l'ETSI⁷⁵, souhaite que les fournisseurs de cloud computing déploient des capacités d'interception légale directement dans la technologie cloud, afin de permettre aux autorités étatiques un accès direct aux contenus stockés par les fournisseurs (y compris email, messages écrits et vocaux)⁷⁶.

4.2.4. « Man-In-The-Middle » (MITM)

Ces attaques sont conçues pour intercepter les données. Cette méthode, pratiquée par exemple au Vietnam⁷⁷, en Iran⁷⁸, peut être mise en œuvre au niveau de l'administrateur du réseau national (le fournisseur d'accès internet).

Selon une étude récente menée par Verify.ly⁷⁹, un très grand nombre d'applications pour iOS mobile sont vulnérables aux attaques MITM⁸⁰, permettant l'interception ou la manipulation des données. Les attaques peuvent notamment être menées par des hackers à portée wi-fi des cibles.

⁷⁴ <https://nsa.gov1.info/utah-data-center/> Le data center de l'Utah est le premier data center de l' [Intelligence Community Comprehensive National Cyber-security Initiative](#) (IC CNCI), qui a pour objectif de répondre aux besoins sans cesse croissant en matière de stockage et traitement des quantités de données traitées par les agences de renseignement américaines. Le projet a pour nom de code Bumblehive. Le centre est opérationnel depuis 2014. Il s'agit là de l'un des plus grands, si ce n'est le plus grand centre de stockage de données de communication au monde.

⁷⁵ L'ETSI (European Telecommunications Standards Institute) est une organisation internationale créée en 1988, regroupant actuellement 800 membres (industriels, universités, opérateurs, administrations, etc.) de 67 pays (<http://www.etsi.org/about/who-we-are> ite consulté le 29 mars 2017), qui travaille à la production de normes/standards dans le domaine des technologies de l'information et de la communication. A l'origine le projet s'inscrivait dans une logique européenne, mais a depuis élargi ses actions au-delà. L'institut a son siège en France, à Sophia Antipolis.

⁷⁶ http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf ETSI DTR 101 567 VO.0.5 (2012-14), Draft Technical Report: Lawful Interception (LI); Cloud/Virtual Services (CLI).

⁷⁷ <http://surveillance.rsf.org/en/vietnam/>

⁷⁸ <http://surveillance.rsf.org/en/iran/>

⁷⁹ <https://verify.ly/#>

⁸⁰ Pierluigi Paganini, 76 Popular iOS apps are vulnerable to man-in-the-middle (MITM) attacks, 7 février 2017, <http://securityaffairs.co/wordpress/56071/mobile-2/mitm-ios-apps.html>

La sécurité des communications dépend des fonctions cryptographiques, mais aussi du protocole d'utilisation de ces fonctions. Dès l'introduction de l'échange de clé Diffie-Hellmann, l'attaque *man-in-the-middle*, montrait que lors d'un échange de clé entre deux correspondants A et B, un intrus situé entre eux pouvait se faire passer par B auprès de A, par A auprès de B, échanger des secrets avec l'un et l'autre, pouvant ainsi intercepter, déchiffrer et rechiffrer les communications qui lui étaient ainsi complètement accessibles. Résister à cette attaque implique de signer les échanges, la signature étant produite à l'aide de la clé privée de l'émetteur, et vérifiée avec sa clé publique.

Cette façon de faire pose immédiatement la question de la validité de la clé publique. Est-elle celle du correspondant légitime ? Ou bien celle de l'intrus ? On entre ici dans une boucle de signatures et de vérification qui a conduit au déploiement des infrastructures à clés publiques (PKI, *Public Key Infrastructure*). La confiance dans une clé publique repose *in fine* sur une autorité de certification reconnue qui signe les clés publiques des usagers.

Si une organisation peut avoir accès aux clés privées des usagers, et la section suivante montre que cette hypothèse n'est pas déraisonnable, l'attaque *man-in-the-middle* est toujours opérante.

Il est toutefois possible que la technologie *blockchain* qui connaît aujourd'hui un grand essor, ne remplace à terme cette infrastructure.

Cet exemple montre que la cryptologie n'est plus l'affaire des acteurs individuels qui souhaitent communiquer discrètement comme au temps du télégraphe, mais est une partie intégrante du système de communication. Or ce système est de plus en plus complexe et fait intervenir de multiples acteurs : systèmes d'exploitation des machines, logiciels applicatifs, fournisseurs d'accès, routeurs du réseau, gestionnaires des matériels câbles et des satellites etc. Le niveau de complexité est arrivé à un point tel qu'aucun acteur ne peut prétendre maîtriser l'ensemble des paramètres qui gèrent la sécurité des communications.

4.2.5. Le DPI (Deep Packet Inspection)

Rappelons que les informations circulent sur le réseau Internet sous forme de paquets de données ou datagramme, constitués d'un entête et d'un bloc de données. L'entête contient des informations sur le destinataire, mais également sur le traitement subi par les données, afin que des dernières parviennent dans leur intégralité au destinataire.

Certaines couches du réseau peuvent réencapsuler les paquets dans d'autres paquets, par exemple pour les fragmenter (partage d'un paquet en deux paquets de taille inférieures), les chiffrer (ajout de données concernant la clé de chiffrement et des données additionnelles dues au chiffrement), les signer (ajout des données d'authentification de l'émetteur), les comprimer, adjoindre des données de correction automatique d'erreur, etc.

L'inspection des paquets en profondeur (DPI, *Deep Packet Inspection*) est l'activité qui consiste à analyser le paquet au-delà de l'entête, et à traiter le bloc de donnée afférent pour en extraire les encapsulations successives et tenter d'aboutir au contenu informationnel final.

L'objectif de ce traitement est de reconnaître la nature du trafic Internet, pour accéder au contenu ou pour en bloquer l'accès. L'objectif peut être avoué comme la gestion des priorités de transmission pour les applications temps réel tels que la voix ou l'image, ou inavoué comme la surveillance des opposants et la censure.

La DPI peut également détecter et contrer certaines attaques en analysant et en détectant le caractère malveillant (virus, vers) ou illégal (pédo-pornographie) de certaines communications.

C'est un outil de DPI (Deep Packet Inspection, analyse en profondeur des paquets), produit par Blue Coat, qui est utilisé par les autorités au Bahrain pour analyser, reconnaître le trafic internet et bloquer l'accès à certains contenus⁸¹. D'autres états comme l'Iran ou la Lybie ont utilisé des équipements de DPI à des fins de surveillance ou de censure (Nokia-Siemens Network en Iran, Amesys en Lybie).

La DPI est un outil qui peut s'avérer très puissant et efficace, mais se heurte aux obstacles suivants :

- Le traitement en profondeur des paquets exige du temps et peut ralentir considérablement le trafic

Le chiffrement des données peut bloquer l'accès aux données et empêcher l'analyse en profondeur.

4.2.6. Les IMSI-Catcher

Les IMSI-Catchers sont des équipements de surveillance qui permettent d'intercepter les communications des téléphones mobiles dans un périmètre limité. A l'origine, il ne s'agissait que de détecter les IMSI (*International Mobile Subscriber Identity*), numéro qui identifie de manière unique un usager afin d'en établir la présence dans le périmètre de propagation des ondes du détecteur. Aujourd'hui, ce terme désigne des équipements qui simulent une antenne-relais et permettent d'intercepter, voire de s'introduire dans le trafic téléphonique.

L'IMSI-catcher s'immisce entre le téléphone mobile de l'utilisateur et l'antenne relais de l'opérateur par une attaque de type *man-in-the-middle*. Lorsqu'ils sont utilisés par les services de renseignement avec la participation des opérateurs, ces équipements peuvent avoir accès aux clés de chiffrement et d'authentification. Dans le cas contraire, ils peuvent exploiter des failles dans les algorithmes de chiffrement. La plus simple est d'imposer l'absence de chiffrement (A5/0) au mobile, de telle sorte que la conversation a lieu en clair. Les attaques cryptographiques existent contre les algorithmes du standard (A5/1), mais nécessitent un accès à un nombre important de données qui peuvent être captées lors d'une communication précédente.

Une propriété contestable de ce type d'équipement est qu'elle cible tous les usagers d'un périmètre donné et non pas seulement la cible identifiée qui fait l'objet d'une surveillance sous contrôle judiciaire.

Des IMSI-Catchers peuvent être réalisés par des amateurs pour une somme modique en utilisant des plateformes génériques de calcul (raspberry-pi) associées à des modules de radio logicielle. Les nouvelles normes de téléphonie mobiles imposent l'authentification des stations de bases par le mobile pour limiter les problèmes de piratage.

4.2.7. Les portes dérobées (backdoors)

Un certain nombre d'affaires récentes comme l'écoute du téléphone portable de la chancelière allemande Angela Merkel par les services états-uniens, ou la controverse entre Apple et le FBI concernant la révélation des clés de chiffrement des données inscrites dans les téléphones portables, montre que la cryptologie est rarement un obstacle insurmontable pour accéder aux contenus.

Même si les clés ont une taille illimitée, il est techniquement possible de leur imposer une entropie⁸² limitée, facilitant une recherche exhaustive par les organisations informées de la malice. Il s'agit là

⁸¹

⁸² L'entropie représente l'effort à faire pour retrouver la donnée par force brutale. Une entropie de 50 bits conduit à une recherche sur 2^{50} éléments.

d'une des possibles portes dérobées (*backdoors*) imposées par les services de renseignement pour pénétrer une cryptologie d'apparence forte. Ces portes dérobées peuvent être réalisées sur le matériel aussi bien que sur le logiciel. Elles sont toutefois plus visibles dans ce dernier cas. Leur existence dans la couche physique est par conséquent plus difficile à établir.

Rappelons que la taille d'une clé est le nombre de symboles binaires nécessaires à son écriture, alors que l'entropie est le nombre de questions avec réponse binaire qu'il est nécessaire de poser pour la déterminer dans son ensemble. Si une clé est constituée de symboles aléatoires et indépendants, l'entropie est égale au nombre de symboles binaires de son écriture, mais il est possible de produire des clés statistiquement indiscernables d'une véritable clé aléatoire, mais ne dépendant que d'un nombre plus réduit de symboles binaires. Il suffira alors aux organisations au fait du procédé d'explorer ce nombre plus réduit de possibilité pour explorer l'espace de toutes les clés produites. Il n'est pas absurde que ce procédé soit effectivement utilisé pour permettre aux services de renseignement de déterminer les clés des équipements de cryptographie exportés vers des pays considérés comme potentiellement non sûrs. Les révélations récentes de l'activité de l'agence de sécurité américaine NSA montrent que ce procédé peut aussi être appliqué aux pays alliés signataires de l'arrangement de Wassenaar.

Un exemple concret de cette pratique est illustré par les résultats obtenus par l'entreprise Cryptosense, spinoff de l'INRIA et publiés sur le site <https://cryptosense.com/an-online-rsa-key-tester/>. Ces travaux font suite à une publication en 2012 d'un article académique, montrant qu'un nombre considérable de clés RSA destinés à assurer la sécurité des communications sur Internet s'avéraient faibles. Rappelons que le RSA est un procédé de chiffrement et de signature à clé publique dont la sécurité repose sur la difficulté de factoriser les grands nombres. En choisissant deux grands nombres premiers p et q , il est possible de publier leur produit $n = p \cdot q$ sans compromettre les facteurs p et q . La fonction de chiffrement ne nécessite que la connaissance du produit n alors que le déchiffrement requiert celle des facteurs p et q .

Les chercheurs de l'UCSD et de l'Université du Michigan ont observé qu'en calculant le pgcd de clés publiques disponibles pour la sécurité SSL/TLS conduisaient à un nombre anormalement élevé de factorisations des clés publiques RSA. Ils ont en effet réussi par ce procédé à factoriser 12 934 clés sur 5 989 923, soit une proportion de 0,22 %. Trois ans plus tard, les clés factorisées étaient de 19 256 sur les 13 603 691 testées, soit environ 0,14%. Obtenir de tels résultats signifie sur les vingt-six millions de nombres premiers générés, on observe près de vingt mille collisions. La formule du paradoxe des anniversaires montre que l'entropie réelle moyenne des nombres premiers produits est d'environ 57 bits. Les nombres premiers utilisés pour générer les clés RSA sont finalement choisis dans un ensemble restreint à 2^{57} nombres. Rappelons que le postulat de Bertrand sur la densité des nombres premiers affirme que le nombre d'entiers premiers de 512 chiffres binaires nécessaires à la production de clés RSA de taille 1024 est de 2^{503} . L'entropie moyenne des clés RSA utilisées sur le réseau Internet pour sécuriser les échanges correspond environ la taille des clés du DES. Explorer 2^{57} est largement accessible aux moyens de calcul actuels. Il est possible que cette faiblesse soit le résultat d'une implémentation défectueuse qui ne respecte pas les règles élémentaires de sécurité en vigueur pour le développement d'applications sécurisées, mais il est aussi possible de soupçonner le caractère intentionnel de cette faiblesse.

La réduction de l'entropie réelle des clés n'est qu'une possibilité d'introduire une porte dérobée dans les fonctions cryptographiques. Lorsque des faiblesses sont découvertes, il n'est jamais impossible d'éliminer la possibilité de leur introduction intentionnelle.

*“As information and communication technologies evolved, so did the means by which States sought to monitor private communications. With increased use of telephones came the use of wiretapping, which consists of placing a tap on a telephone wire to listen to private phone conversations. With the replacement of analogue telephone networks with fibre optics and digital switches in the 1990s, States redesigned the networking technology to include **interception capabilities (“backdoors”)** to*

*permet State surveillance, rendering modern telephone networks remotely accessible and controllable*⁸³.

La liberté d'utiliser la cryptographie librement contrarie les Etats dans leur mission de surveillance pour lutter contre les organisations criminelles ou terroristes. Cette tension entre liberté et contrôle est manifeste dans de nombreux documents officiels. La réglementation en matière de cryptologie de 1991 édictée par le SCSSI (Services Centraux pour la Sécurité des Systèmes d'Information, ancêtre de l'ANSSI) énonçait en 1991 :

*« Dans le cadre de la protection des personnes et des biens, de la sécurité intérieure et de la défense nationale, l'État doit mettre en place des mesures nécessaires pour éviter que ces technologies (celles de l'information et de la communication) ne facilitent en toute impunité et en toute discrétion, le développement d'actions ou de trafics illégaux (petite et grande délinquance, terrorisme, mafia, pédophilie, blanchiment d'argent, fraudes financières, espionnage industriel, ...) »*⁸⁴

La question se pose sur la nature de ces « mesures nécessaires » pour rendre accessible aux services qui en ont besoin le contenu des échanges protégés avec une cryptologie forte. Une première solution avait été de limiter la taille des clés de manière à rendre accessible la recherche exhaustive par les institutions dotées de puissants moyens de calcul. La taille des clés informait d'ailleurs sur la puissance de ces moyens selon les réglementations des pays. Alors que la France limitait l'usage des clés à 40 bits, les États-Unis autorisaient 56 bits.

Cette solution a l'inconvénient rédhibitoire d'affaiblir pour tous la protection, y compris pour les échanges où cette protection est pleinement justifiée, comme par exemple lors des négociations de contrats ou les échanges commerciaux.

Une deuxième solution est d'introduire dans le système cryptographique des « portes dérobées » (*backdoor*) inconnues des usagers, mais connues des services autorisées. Il existe des solutions mathématiques pour rendre ces portes dérobées sûres, par exemple chiffrer les clés de chiffrement avec une clé publique, de telle sorte que seul l'état dépositaire de la clé privée correspondante puisse accéder au déchiffrement et finalement aux échanges en clair.

Cette solution a été largement contestée par l'ensemble des acteurs de la cryptologie⁸⁵ ;

« Whitfield Diffie, l'un des créateurs du protocole Diffie-Hellman pour l'échange sécurisé de clés, a déclaré lors d'une conférence (...):

- *La porte dérobée mettrait les fournisseurs dans une position difficile avec les autres gouvernements et les clients internationaux, affaiblissant sa valeur.*
- *Ceux qui veulent cacher leurs conversations au gouvernement pour des raisons néfastes peuvent facilement contourner la porte dérobée.*
- *Les seules personnes qui seraient faciles à surveiller seraient en premier lieu les personnes qui ne se soucient pas de la surveillance gouvernementale.*

⁸³ http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

⁸⁴ texte reproduit sur <http://securinet.free.fr/crypto-regle-fr.html>

⁸⁵ <https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/>

- *Il n'y a aucune garantie que quelqu'un d'autre ne puisse exploiter la porte dérobée pour ses propres fins ».*

Les portes dérobées officielles, comme le clipper chip mis en place sous le gouvernement Clinton a finalement été rejeté. Ce rejet des méthodes officielles n'a semble-t-il pas découragé les états à mettre en place de toutes façons une solution. Le contournement de la cryptologie n'étant pas officiel, il se trouve impensé, et dissimulé à travers des failles régulièrement découvertes dans les systèmes.

La question des portes dérobées se trouve relancée par une lettre adressée par les ministères de l'intérieur français et allemands à la commission européenne. Dans cette lettre en date du 20 février 2017, signée par Thomas de Maizière et Bruno Leroux, ministres de l'intérieur des deux pays⁸⁶, il est écrit :

« La lutte contre le terrorisme requiert de donner les moyens juridiques aux autorités européennes afin de tenir compte de la généralisation du chiffrement des communications par voie électronique lors d'enquêtes judiciaires et administratives. La commission européenne doit veiller à ce que des travaux techniques et juridiques soient menés dès maintenant pour étudier la possibilité de définir de nouvelles obligations à la charge des prestataires de services de communication par voie électronique tout en garantissant la fiabilité de systèmes hautement sécurisés et de proposer sur cette base une initiative législative en octobre 2017.

D'une manière générale, la Stratégie de cybersécurité de l'UE de 2013 doit être révisée pour inclure de nouvelles actions et établir un état des lieux des mesures qu'il reste encore à prendre.

Pour prévenir et dissuader toute forme de menace terroristes, nous soutenons la démarche de la Commission consistant à mettre à jour l'agenda relatif aux menaces chimiques, biologiques et radionucléaires (CBRN) afin d'améliorer les mesures nécessaires pour prévenir, lutter et réduire ces menaces. Cette modernisation est essentielle pour adapter la réponse des Etats membres aux évolutions technologiques permanentes. Cet agenda doit être conduit en partenariat avec le Centre européen de lutte contre le terrorisme (ECTC) d'Europol ».

Il s'agit clairement de relancer l'idée d'une introduction de portes dérobées dans les solutions de chiffrement pour rendre accessible les contenus dans le cadre d'opérations qui le nécessiteraient. Cette proposition a reçu l'opposition de nombreux intervenants.

La CNIL en particulier, milite pour une cryptographie forte, sans porte dérobée et maîtrisée par les utilisateurs, arguant de l'existence de dispositifs juridiques contraignant pour fournir les clés de chiffrement. Un document en date de 2016 énonce :

« Les limites de l'usage de portes dérobées

L'actualité récente a conduit à un débat sur la pertinence de l'introduction, par le droit national, de portes dérobées (backdoors) ou d'une clé maitre permettant in fine d'accéder à des données contenues dans un système protégé par une solution de chiffrement présentée comme à la main de l'utilisateur. Un tel dispositif soulèverait de nombreuses questions :

⁸⁶

https://regmedia.co.uk/2017/02/28/french_german_eu_letter.pdf
<https://fr.scribd.com/document/340506340/2017-02-17-De-claration-FR-DE-II-Officielle>,

et

- *il créerait un risque collectif tendant à affaiblir le niveau de sécurité des personnes face à l'ampleur du phénomène cybercriminel, alors qu'il n'empêcherait pas, techniquement, des personnes malveillantes de continuer à utiliser des solutions de chiffrement à titre individuel pour protéger la confidentialité de leurs communications et de leurs données stockées ;*
- *il serait vraisemblablement peu robuste dans le temps, face aux attaques des États ou du crime organisé, d'autant plus qu'il serait nécessaire d'échanger entre autorités le secret ou les clés ;*
- *il serait très complexe à mettre en œuvre, de manière sûre, alors que les applications sont globalisées et mondialisées.*

Les solutions de chiffrement robustes, sous la maîtrise complète de l'utilisateur, contribuent à l'équilibre et à la sécurité de l'écosystème numérique. L'introduction de portes dérobées ou de clés maîtres conduirait à affaiblir la sécurité des solutions techniques aujourd'hui déployées, ce qui serait préjudiciable au patrimoine informationnel des entreprises, à la stabilité de l'écosystème de l'économie du numérique et à la protection des libertés des personnes.

En conséquence, la CNIL considère que⁸⁷ :

- *le chiffrement contribue à la résilience de nos sociétés numériques et de notre patrimoine informationnel ;*
- *dans le cadre des procédures judiciaires, il existe déjà de nombreuses voies permettant aux autorités d'accéder et d'analyser les contenus intéressant l'enquête ou utiles à la manifestation de la vérité ;*
- *les personnes mises en cause et les tiers ont obligation de coopérer avec les autorités ;*
- *la mise en place de portes dérobées ou de clés maîtres fragiliserait l'avenir de l'écosystème du numérique. »*

Guillaume Poupard, directeur de l'ANSSI développe une position semblable. Il s'est prononcé (janvier 2016) contre tout accès parallèle aux contenus qui serait inséré par les fournisseurs de technologie, et se prononce pour les techniques d'enquêtes intrusives permettant d'intercepter les messages avant et/ou après leur chiffrement⁸⁸.

Les industriels américains du CCIA, association qui regroupent les principales entreprises des technologies de l'Internet aux Etats-Unis, incluant en particulier Amazon, Google, ebay, Microsoft, Netflix, et bien d'autres, s'opposent également à toute méthode qui conduirait à introduire un chiffrement faible dans les équipements.

"It remains unclear exactly how online service providers should provide law enforcement authorities with access to end-to-end encrypted user data. Any backdoors to encrypted data would pose serious risks to the overall security and confidentiality of Europeans' communications, which seems inconsistent with existing legal protections for personal data. Weakened security ultimately leaves online systems more vulnerable to all types of attacks from terrorists to hackers. This should be a time to increase security—not weaken it"⁸⁹.

⁸⁷ <https://www.cnil.fr/fr/les-enjeux-de-2016-3-quelle-position-de-la-cnil-en-matiere-de-chiffrement>

⁸⁸ <http://hightech.bfmtv.com/internet/l-anssi-ne-croit-ni-a-l-os-souverain-ni-aux-portes-derobe-es-946311.html>

⁸⁹ <http://www.ccianet.org/2017/02/is-europe-about-weaken-encryption/>

L'Enisa (European Union Agency for Network and Information Security) a une position semblable⁹⁰ (décembre 2016):

“ENISA sees that:

- *The use of backdoors in cryptography is not a solution, as existing legitimate users are put at risk by the very existence of backdoors.*
- *Backdoors do not address the challenge of accessing of decrypting material, because criminals can already develop and use their own cryptographic tools. Furthermore, new technologies are now being deployed making lawful interception in a timely manner very difficult.*
- *Judicial oversight may not be a perfect solution; as different interpretations of the legislation may occur.*
- *Law enforcement solutions need to be identified without the use of backdoors and key escrow. It is very difficult to restrict technical innovation using legislation.*
- *History has shown that technology beats legislation, and criminals are best placed to capitalise on this opportunity.*
- *The perception that backdoors and key escrow exist, can potentially affect and undermine the aspirations for a fully embraced Digital Society in Europe.*
- *History has shown that legal controls are not always successful, and may harm and inhibit innovation, as seen with previous US experience”.*

4.3. Surveiller les e-mails

L'entreprise Yahoo ! se serait conformée aux demandes du gouvernement pour procéder à la surveillance des emails de ses utilisateurs⁹¹. Dans la même période des centaines de millions de comptes ont également été piratés. Y a-t-il un lien entre ces deux affaires, d'un côté une pratique de l'entreprise, de l'autre une pratique (le hacking) subie par l'entreprise ? Dans le premier cas les utilisateurs ignorent bien sûr faire l'objet de cette surveillance, et dans le second cas à la fois l'entreprise et ses utilisateurs ignorent être victimes de piratage. On voit ici que dans le même temps, sur les mêmes objets, peuvent s'exercer cybersurveillance et hacking.

La cybersurveillance des utilisateurs par Yahoo ! est contraire à la législation américaine qui n'autorise que la surveillance des communications étrangères. L'obligation imposée à Yahoo ! par les autorités américaines est révélatrice de la pression que s'autorisent d'exercer ces dernières sur l'industrie américaine, et des libertés qu'elles s'accordent avec le cadre légal (ici toutes les communications sont scannées, et non pas seulement celles d'étrangers). L'entreprise est cependant soucieuse de son image, consciente que cette collaboration avec les autorités, qu'elle ne semble guère en mesure de refuser, pénalise son business, son image de marque, sa réputation, etc.

Les piratages massifs dont elle est victime, révélées fin 2016, ajoutent à cette atteinte à l'image. Vers le 20 octobre 2016, Yahoo demandait au patron du renseignement américain la divulgation de l'ordre envoyé par les autorités⁹². L'affaire fut médiatisée alors que Yahoo négociait un rachat par Verizon, qui aurait saisi l'opportunité de la situation pour demander une baisse de prix.

⁹⁰ The importance of cryptography for the digital society, décembre 2016, <https://www.enisa.europa.eu/news/enisa-news/the-importance-of-cryptography-for-the-digital-society>

⁹¹ « Selon des anciens employés, l'entreprise a accepté de jouer à Big Brother... », 5 octobre 2016, <http://www.20minutes.fr/high-tech/1936339-20161005-yahoo-accuse-avoir-espionne-emails-tous-utilisateurs-gouvernement-americain>

⁹² Juha Saarinen, Yahoo pleads with US govt to clarify email spying order, 20 octobre 2016, <https://www.itnews.com.au/news/yahoo-pleads-with-us-govt-to-clarify-email-spying-order-439744>

4.4. Les messageries sécurisées

L'offre en matière d'applications de messagerie sécurisée est pléthorique. Une étude comparative de l'EFF en recense près de 40⁹³ en 2016 au rang desquelles : AIM, BlackBerry Messenger, BlackBerry Protected, ChatSecure+ Orbot, Ebuddy XMS, Facebook chat, FaceTime, Google Hangouts/Chat « off the record », Hushmail, iMessage, iPGMail, Jitsi+Ostel, Kik Messenger, Mailvelope, Mxit, Off-the-Record (OTR) Messaging for Windows (Pidgin), PGP for Mac (GPGTools), PGP for Windows Gpg4win, QQ, RetroShare, Signal/Redphone, Silent Phone, Silent Text, Skype, SnapChat, StartMail, SureSpot, Telegram, TextSecure, Threema, Viber, Virtru, WhatsApp, Wickr. Mais on peut bien sûr ajouter quantité d'autres applications à cette liste : Protonmail⁹⁴, Meebo, Imo.IM, Pidgin...

Le développement des messageries sécurisées comme Telegram, WhatsApp, Skype, Facebook, pose de nouveaux problèmes en termes d'interception.

D'une part elles gênent le travail de l'intercepteur en masquant certaines métadonnées. Le paquet est à destination du service de messagerie. Le véritable destinataire étant inclus dans la partie chiffrée du paquet, il n'est pas directement accessible à l'intercepteur.

D'autre part, les messageries sécurisées, chiffrées (notamment celles qui le sont de bout en bout), ne sont en vérité pas toutes aussi sécurisées qu'il n'y paraît. Nombre de messageries sécurisées sont vulnérables aux cyberattaques.

Les controverses apparues autour de ces messageries non contrôlées par les US, comme Skype avant le rachat par Microsoft ou Telegram éclairent cette dualité.

Nom de l'application	Origine de l'application	Quelques caractéristiques
WeChat	Asie (Chine)	Les données échangées sont chiffrées entre les clients et les serveurs de Tencent. Mais les messages dont les utilisateurs sont enregistrés avec des numéros de téléphone chinois, sont contrôlés (censure exercée sur les messages qui critiquent le régime)
Kakao Talk	Asie (Corée du Sud)	Chiffrement (algorithme asymétrique) Chiffrement non disponible pour les appels passés depuis l'application Le chiffrement n'est pas activé par défaut Il n'est pas possible de spécifier la durée de vie des messages chiffrés Les messages sont stockés sur les serveurs de l'entreprise pendant 2 à 3 jours
Line	Asie (Japon)	Chiffrement de bout en bout avec le protocole ECDH (Eliptic Curve Diffie-Hellman) Les messages stockés sur serveurs Line sont chiffrés Pas d'autodestruction des messages stockés En Chine, l'application remplace automatiquement certains mots par des astérisques = censure
WhatsApp Messenger	USA	Entreprise rachetée par Facebook en 2014 Change ses conditions d'utilisation en 2016 et partage les données avec les réseaux sociaux Les données échangées par les utilisateurs sont chiffrées
Facebook Messenger	USA	Les conversations ne sont pas chiffrées par défaut Les conversations chiffrées le sont avec Signal

⁹³ <https://www.eff.org/node/82654>

⁹⁴ <https://protonmail.com/fr/>

		Autodestruction des messages Une conversation chiffrée n'est accessible qu'à partir du terminal depuis lequel elle a été initiée
--	--	---

Tableau : quelques applications de messagerie et commentaires sur leur niveau de sécurité⁹⁵.

4.4.1. MinInt(F) versus messageries sécurisées

L'Etat français versus les fournisseurs de logiciels de communications électroniques.

- « Chiffrement. L'intérieur veut obliger Skype à procéder à des interceptions »⁹⁶. Pour lutter contre les messages chiffrés sur ADSL, 3G, 4G, téléphonie mobile, l'Intérieur a envisagé d'exiger une mise au clair des informations chiffrées, de Skype, Viber, Whatsapp, Facebook, Gmail, Twitter, Kik, Wechat. « Leur mise au clair en revanche s'avère impossible ou trop longue même avec les moyens sophistiqués utilisés par certains services spécialisés ». L'Intérieur envisage donc deux scénarios :
 - L'un est temporaire, et vise à « **obtenir des fournisseurs de logiciels de communications électroniques** (Skype, Viber, Whatsapp, Facebook, Gmail, Twitter, Kik, Wechat, etc.) **des clés ou des algorithmes de déchiffrement** afin de pouvoir mettre au clair, presque en temps réel, les flux internet interceptés, et de les sanctionner sur le plan pénal ou administratif en cas d'absence de réponse ».
 - l'autre passerait par une modification de la loi (Code des Postes et Télécommunications Electroniques) **pour contraindre les fournisseurs de logiciels de communications électroniques à procéder à des interceptions** et fournir en temps réel et en clair les données aux autorités (règles qui s'imposent déjà aux opérateurs de télécommunications).

4.4.2. BlackBerry, l'application BBM et les Etats

L'application BlackBerry messenger ("BBM") permet d'envoyer des messages chiffrés.

Faits	Date
Le SGDSN demande au président N. Sarkozy de ne plus utiliser son BlackBerry parce que les contenus des conversations sont accessibles sur des serveurs basés à l'étranger	2007
Les Etats se sentent démunis face à cette messagerie chiffrée. Ils font donc pression directement sur l'entreprise : l'Arabie Saoudite a coupé brièvement les services BBM. Rapport de force entre l'entreprise canadienne RIM et les Etats qui peuvent lui bloquer des marchés. C'est donc un rapport de force entre politique (sécurité, lutte contre le terrorisme, contre l'insurrection...), commerce, valeurs...	2010
RIM aurait conclu un accord avec le gouvernement de l'Inde permettant aux autorités du pays d'accéder en clair aux contenus échangés par les utilisateurs du BlackBerry.	2010
D'après les informations révélées par E. Snowden, la NSA aurait contourné la protection cryptographique des BlackBerry en 2010 ⁹⁷	2010
L'application BBM fait la une de l'actualité en août 2011 après que Mark Duggan, un jeune britannique, ait	2011

⁹⁵ Tableau reconstitué d'après des données relevées dans le numéro 90 (mars/avril 2017) de la revue MISC dont le dossier est consacré aux messageries sécurisées.

⁹⁶ <http://www.nextinpact.com/news/101236-chiffrement-l-interieur-veut-obliger-skype-a-proceder-a-interceptions.htm>

⁹⁷ Lucas Atkins, How the NSA Reportedly Intercepted BlackBerry Communications, 9 septembre 2013, <http://n4bb.com/nsa-reportedly-intercepted-blackberry-communications/>

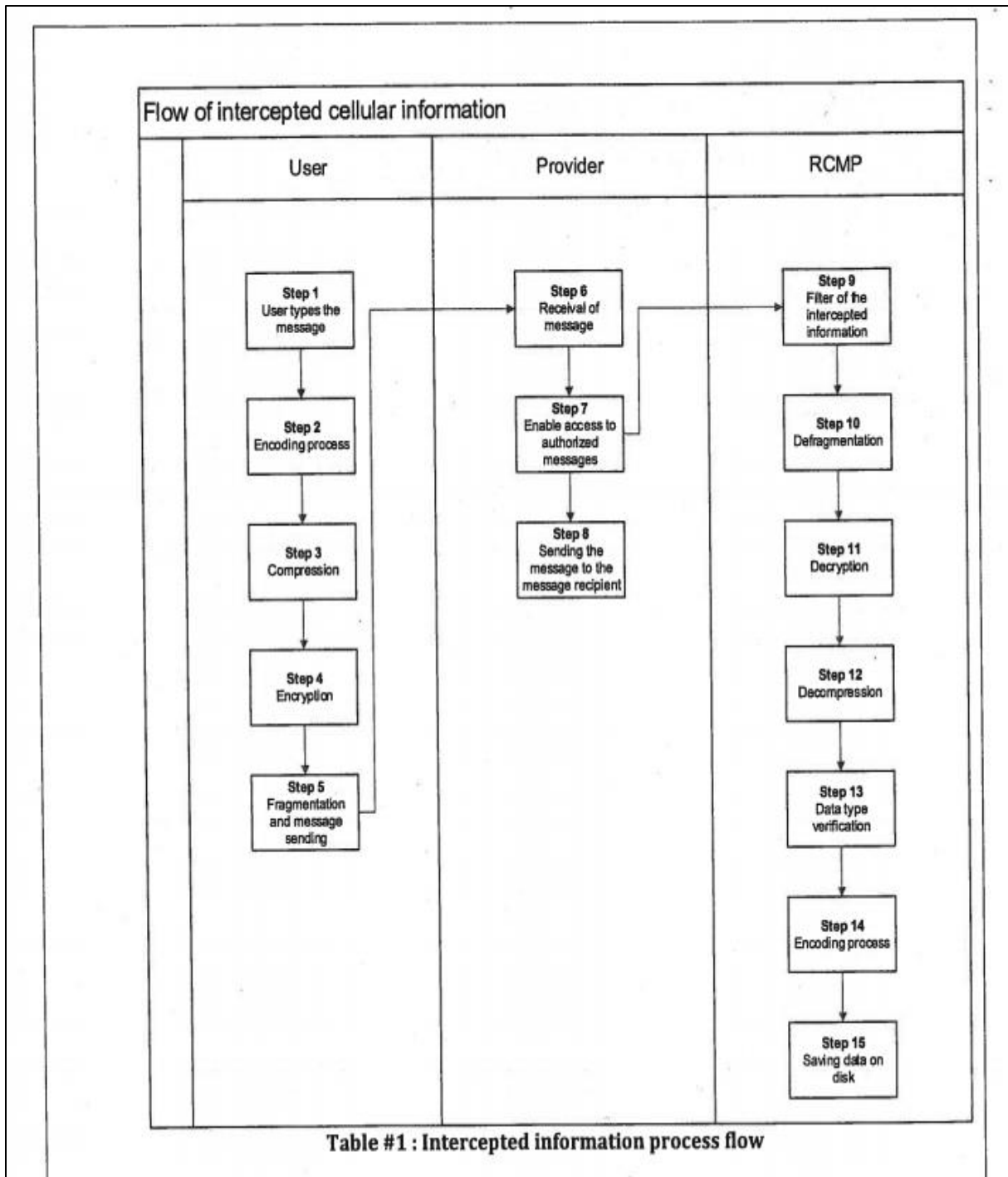
envoyé à sa petite amie à l'aide de l'outil un bref message : « les flics me poursuivent ». La mort de Mark Duggan fut à l'origine des émeutes de Tottenham ⁹⁸ . Le BlackBerry fut alors considéré comme l'un des instruments ayant facilité la coordination des émeutiers.	
Opération « Project Clemenza » contre la mafia, durant laquelle la police canadienne a intercepté plus d'un million de messages de BlackBerry ⁹⁹ .	2010-2012

Comment fonctionnait l'application BBM ?

- Elle permettait l'envoi de messages gratuits et chiffrés
- Les messages transitait sur internet
- Les serveurs accueillant les informations se trouvaient au Canada, Etats-Unis, Royaume-Uni
- Pour communiquer avec cette application, les deux correspondants devaient au préalable échanger un code personnel

⁹⁸ Geoffrey Le Guilcher, "Pourquoi le Blackberry rend-il es gouvernements paranos ? », 10 août 2011, <http://www.lesinrocks.com/2011/08/10/actualite/pourquoi-le-blackberry-rend-il-les-gouvernements-paranos-1111190/>

⁹⁹ Jordan Pearson & Justin Ling, Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages, 14 avril 2016, https://motherboard.vice.com/en_us/article/rcmp-blackberry-project-clemenza-global-encryption-key-canada



Source : https://motherboard.vice.com/en_us/article/rcmp-blackberry-project-clemenza-global-encryption-key-canada

Dans ce diagramme, publié sur le site Motherboard¹⁰⁰, est présentée l'organisation du système d'interception des communications des Blackberry par la RCMP (Royal Canadian Mounted Police) lors de l'opération Clemenza. Le système implique que la police canadienne était en mesure de déchiffrer les messages. Dans ces situations, la question de fond qui demeure, pour les utilisateurs, est celle du degré d'implication, de collaboration de l'industriel avec les forces de sécurité des Etats. Les

¹⁰⁰ https://motherboard.vice.com/en_us/article/rcmp-blackberry-project-clemenza-global-encryption-key-canada

industriels eux-mêmes ne sont guère enclins à avouer ces collaborations, en raison de l'impact négatif sur la clientèle : « *it is not a good marketing thing to say we work with the police* »¹⁰¹. En complément à ces interceptions de messages la police canadienne a utilisé lors de l'opération Clemenza des IMSI-catchers (pratiques qui semblent remonter à plusieurs années, car l'article mentionne une formation à l'utilisation de l'IMSI-catcher reçue par les policiers en 2005).

4.5. L'interception des communications dans les lieux publics

Une note de l'OSAC (Overseas Security Advisory Council)¹⁰² reprenant des notes du Département d'Etat des Etats-Unis met en garde les touristes américains contre l'utilisation des connexions wi-fi gratuites non-sécurisées dans les lieux publics français :

- *"Cybersecurity Issues Wi-fi hot spots should not be trusted; criminals will configure "man-in-the-middle" access points that appear free so that they can intercept communications from anyone who connects. This allows hackers to access sensitive information appearing on the user's screen. It also provides a mechanism by which a hacker can gain control of the connecting device. Owners of public Internet cafes may install key logging software that enables theft of sensitive information. Smart phones and computers, but specifically Apple products, cost more in France than in the U.S. and are targeted by local petty thieves. Be wary of where your laptop or smart phone is used or stored. France has a capable national police force; however, transnational organized crime (TOC) operatives reside in France. TOC syndicates are technically savvy and conduct many of their schemes via cyber platforms"*.¹⁰³

4.6. Internet, un réseau de câbles

Selon les informations fournies sur le site Telegeography¹⁰⁴ :

- Début 2017, il y aurait 428 câbles internet sous-marins pour une longueur totale de plus de 1 millions de kilomètres. La difficulté du décompte tient à l'évolution permanente de cet énorme réseau planétaire : de nouveaux câbles sont déployés, d'autres sont enlevés. La longueur des câbles est très variable : d'une centaine de kilomètres à plus de 20 000 kilomètres.
- Les câbles ont une signification du seul fait de leur existence. *"Undersea cables are built between locations that have something "important to communicate."*¹⁰⁵ Ainsi selon le site l'absence de câble direct entre l'Australie et l'Amérique du Sud signifie que les deux continents n'ont pas besoin d'échanger beaucoup de données.
- Les câbles sous-marins utilisent la technologie de fibre optique.
- Les cartographies que l'on peut généralement trouver sur internet¹⁰⁶ schématisent les chemins empruntés par les câbles. Il ne s'agit donc pas toujours de la véritable route empruntée. Ce que les cartes tiennent à montrer c'est 1/ l'existence d'un câble, et 2/ les points de départ et d'arrivée.

¹⁰¹ https://motherboard.vice.com/en_us/article/rcmp-blackberry-project-clemenza-global-encryption-key-canada

¹⁰² <https://www.osac.gov/Pages/Home.aspx>

¹⁰³ France 2017 Crime & Safety Report , OSAC, 6 février 2017, <https://www.osac.gov/pages/ContentReportPDF.aspx?cid=21206>

¹⁰⁴ <http://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions> Site consulté le 10 mars 2017.

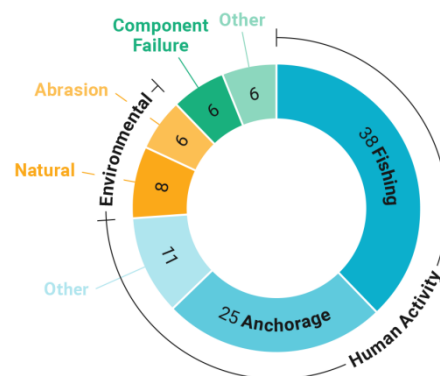
¹⁰⁵ <http://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions>

¹⁰⁶ Exemple : <http://www.submarinecablemap.com/>

- Les pays qui disposent de côtes maritimes sont pratiquement tous connectés et disposent alors de plusieurs câbles (afin d'assurer une continuité de service dans le cas d'un accident sur l'un des câbles).
- Le réseau de fibre optique est fragile : une fibre optique est, seule, extrêmement fragile, car du diamètre d'un cheveu humain. Les fibres sont donc protégées, enveloppées de couches de plastique et parfois de fil d'acier. Malgré les précautions prises dans l'installation des câbles, le choix des zones de déploiement, la solidité physique des câbles conçus pour résister aux conditions météorologiques extrêmes, on recense une centaine de coupures de câbles chaque année. Les câbles sont posés au fond des mers et près des côtes ils sont enterrés pour éviter les accidents. Pour leur protection physique, matérielle, les câbles sont installés dans les océans en prenant compte de différents facteurs.
- Les câbles sont la propriété d'opérateurs de télécommunications. Mais depuis quelques années les fournisseurs de contenus (content providers) investissent de plus en plus dans le câble (Google, Facebook, Microsoft, Amazon, etc.)
- La nécessité d'accroître la bande passante des réseaux justifie les investissements dans le câble.
- Le câble n'est pas concurrencé par les satellites qui n'ont pas la capacité de traiter des volumes de données aussi importants (les nouveaux câbles seraient capables de traiter quelques 160 Terabits par seconde). Toujours selon le même site Telegeography, une statistique récente indique qu'actuellement seul 0.37% du trafic de l'internet mondial passerait par les satellites. Les communications des téléphones portables elles-mêmes transitent par les câbles terrestres et sous-marins. Seule la transmission entre le téléphone et les émetteurs/récepteurs de la téléphonie mobile sont wireless. Les investissements des grandes compagnies dans le satellite voire les drones ont pour objectif d'apporter internet dans les zones qui ne peuvent accéder aux réseaux câblés.

La question de l'interception des communications satellitaires est-elle donc toujours pertinente ?

Quelques coupures de câbles sous-marins restent inexplicées, ne sont en tous cas pas documentées :



Source : <http://www2.telegeography.com/hs-fs/hubfs/2017/submarine-cable-map/faq-graphics/causes-of-cable-faults.png?t=1489083125351&width=1055&name=causes-of-cable-faults.png>

Les services de renseignement de certains pays (USA, UK...) interceptent les communications des câbles sous-marins et terrestres. Le GCHQ verse plusieurs millions de livres aux opérateurs (Telco BT,

Vodafone...) pour se connecter aux infrastructures câbles¹⁰⁷. Les agences de renseignement peuvent également installer des équipements d'interception chez des opérateurs sans leur autorisation, sans en informer les propriétaires des réseaux câblés.

V – Protéger les communications contre les risques d'interception

L'interception fait face à des résistances de diverses natures. Il y a tout d'abord celles de nature technique, voire physiques (certains signaux par exemple ne peuvent être interceptés dans tous les environnements ; il ne peut pas y avoir interception lorsque une cage de Faraday¹⁰⁸ fait barrage au signal, etc.) Mais il y a aussi les résistances déployées par les cibles des interceptions, qui vont faire preuve d'imagination pour faire obstruction, échapper à l'interception, compliquer la tâche voire la rendre impossible : chiffrer les communications fait bien sûr partie de ces stratégies. D'autre part, le droit, lorsqu'il encadre les pratiques, est d'une certaine manière aussi un frein car il vise à protéger la société, les individus, contre des pratiques abusives.

Dans ce chapitre nous nous intéressons plus particulièrement à la cryptographie, comme moyen de protection des communications et résistance opposée aux capacités d'interception.

5.1 - La cryptographie

La cryptographie est aujourd'hui un art suffisamment développé et mûr pour assurer la définition de fonctions de chiffrement ou d'authentification dont le niveau de sécurité rend inaccessible à un adversaire le contenu des messages et lui nie la possibilité de forger une fausse signature. Les fonctions cryptographiques utilisées dans les standards sont aujourd'hui assorties de preuves de sécurité admises par la communauté scientifique.

L'accès aux contenus des communications chiffrées ne peut plus se contenter de l'attaque des fonctions cryptographiques, celles-ci ayant atteint un niveau de sécurité qui les rend impénétrables, mais davantage sur leur contournement ou sur l'exploitation de faiblesses dans leur mise en œuvre.

La cryptographie est une technique destinée à rendre incompréhensible les données échangées sans la connaissance d'une clé secrète partagée par les correspondants. Des mécanismes appelés à *clé publique* permettent de localiser la clé secrète uniquement chez le destinataire.

Ces procédés ont connus un essor considérable durant la seconde guerre mondiale et le travail mené par l'équipe de Bletchley Park pour accéder au contenu des messages chiffrés allemand a considérablement contribué à la victoire des Alliés.

Comme la cryptographie rend en théorie vaine toute interception, ces techniques ont été, jusque dans les années 2000, réservées aux communications justifiant d'une sensibilité critique (militaires, diplomates, industries de défense, industries sensibles) et interdite aux particuliers. Les moyens cryptographiques étaient alors considérés comme des armes au même titre que les munitions, et leur détention non autorisée était passible de sanctions pénales.

Le développement du réseau Internet et en particulier celui du commerce électronique rendait intenable le maintien d'une législation trop restrictive.

Les années 1990-2000 ont vu une tension entre les tenants d'un contrôle de la cryptographie par les États et les tenants d'une libéralisation complète. Ces derniers ont finalement obtenu gain de cause.

La « loi pour la confiance dans l'économie numérique » du 21 juin 2004 affirme dans son article 30 que :

¹⁰⁷ <http://www.duncancampbell.org/content/gchqs-middle-east-cable-tap-centre-revealed>

¹⁰⁸ Lorsque la source est confinée dans une enceinte métallique étanche, les ondes électromagnétiques ne se diffusent pas à l'extérieur, provoquant une isolation communicationnelle.

« L'usage des moyens de cryptographie est libre ».

La recrudescence des attentats terroristes relance l'idée d'une cryptographie contrôlée par les états afin de donner aux services de police et de renseignement les moyens d'accéder au contenu des messages échangés par les individus surveillés.

Les progrès de l'art cryptologique conduisent aujourd'hui à des procédés théoriquement inviolables.

L'accès au contenu en clair est prouvé impossible sans la connaissance des clés secrètes.

L'accès au contenu de communications chiffrées par les services de sécurité américains (NSA *National Security Agency*) montre que les systèmes cryptographiques déployés dans les systèmes de communication actuels (téléphonie mobile, mails) ne satisfont pas les hypothèses de caractère aléatoire et secret des clés utilisés.

L'existence de portes dérobées (*Backdoors*) destinées à rendre les clés de chiffrement accessibles aux services de renseignements ne fait plus aucun doute dans des systèmes fournis par des grands opérateurs industriels, tous américains, de l'industrie numérique actuelle (GAFAM, *Google Apple Facebook Amazon Microsoft*). Revenu dans le giron de *Microsoft*, le logiciel de téléphonie sur Internet *Skype* suscite bien moins de craintes de la part des services que lorsqu'il était sous le contrôle de son concepteur lituanien.

Bien que d'usage civil libre, la cryptographie fait toujours partie des « technologies à double usage », et à ce titre, les pays signataires de l'arrangement de Wassenaar¹⁰⁹ s'engagent à :

*«... s'assurer que les transferts d'armements conventionnels et de biens et technologies à double usage qu'ils effectuent ne contribuent pas au développement ou au renforcement de capacités militaires pouvant nuire à la sécurité et à la stabilité régionales et internationales ».*¹¹⁰

Il est donc fort probable que les produits de chiffrement sont contrôlés par les services de renseignements des États dans lesquels ils sont produits.

Le mouvement du logiciel libre, et en particulier le mouvement d'inspiration anarchiste *cypherpunk*¹¹¹ revendique la protection de la vie privée de chaque citoyen en s'appuyant sur une cryptographie libre produite par des développeurs indépendants non soumis aux impératifs de contrôles des États.

5.2 - La stéganographie

La stéganographie est un procédé de camouflage du message lui-même. L'information utile au destinataire est camouflée dans un objet, dans un dessin, voire dans un autre texte. Il s'agit d'un procédé très ancien, décrit en particulier par Enée le Tacticien dans son traité sur la défense des places¹¹². On trouve de multiples exemples en littérature et en art. Il s'agit d'un procédé très prisé des espions en temps de guerre. David Kahn¹¹³ [KAH], rapporte le cas de cet espion allemand en

¹⁰⁹ <http://www.wassenaar.org>

¹¹⁰ <http://www.delegfrance-onu-vienne.org/Arrangement-de-Wassenaar-971>

¹¹¹ <http://www.activism.net/cypherpunk/manifesto.html>

¹¹² <http://remacle.org/bloodwolf/erudits/enee/defensesdesplaces.htm>

¹¹³ David Kahn, *The Code Breakers*, Scribner, 1996

activité aux états unis pendant la première guerre mondiale qui fait transmettre deux dépêches pour passer un message secret à ses supérieurs :

President's embargo ruling should have immediate notice, grave situation affecting international laws. Statement fore-shadows ruin of many neutral. Yellow journals unifying national excitement immensely¹¹⁴.

Et :

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils¹¹⁵.

Le véritable sens de ces dépêches apparaît lorsqu'on extrait les premières de chaque mot dans la première dépêche et la seconde lettre de chaque mot dans la seconde (*Pershing sails from NY June 1*, Pershing embarque de NY le 1^{er} juin). L'espion indique la date de départ du général Pershing après la constitution du corps expéditionnaire américain en Europe suite à l'entrée en guerre des États-Unis le 6 avril 1917¹¹⁶.

La stéganographie est utilisée de nos jours pour inscrire des informations de droit d'auteur dans les œuvres artistiques numérisées. Elle semble rester un procédé très utilisés par les réseaux terroristes en raison de la grande discrétion et de la difficulté à la contrecarrer.



Fig. 1: Un exemple de stéganographie dans *Le Lotus Bleu* de Hergé (1934)

114 La décision d'embargo du président devrait avoir effet immédiat. Situation sérieuse mettant en cause les lois internationale. Cette déclaration présage la ruine de nombreux pays neutres. La presse à sensation unifie énormément le sentiment national.

115 Apparemment, la protestation des pays neutres est totalement écartée et ignorée. Isman frappe fort. L'issue du blocus donne le prétexte pour un embargo sur certains produits, sauf suifs et huiles végétales.

116 Contrairement à ce que semble avoir appris notre espion, Pershing a quitté New-York le 28 mai 1917 et non pas le 1^{er} juin.

5.3. - Le calcul quantique

La sécurité des systèmes cryptographiques reposent sur des problèmes réputés difficiles, comme la factorisation des entiers. Autant multiplier deux nombres, même très grands, ne pose aucun problème aux ordinateurs actuels qui peuvent effectuer cette opération sur des nombres de plusieurs milliers de chiffres en une fraction de seconde, autant l'opération inverse, à savoir la factorisation, est une opération difficile pour laquelle on ne connaît pas à ce jour d'algorithme efficace. Un écolier peut facilement calculer 19×13 . Mais trouver les facteurs de 247 demande un certain travail. La dissymétrie entre les difficultés de la multiplication et de la factorisation augmente avec la taille des nombres considérés.

Le système cryptographique RSA exploite cette dissymétrie. La clé privée consiste en deux grands nombres premiers, et la clé publique est leur produit. Il est aujourd'hui pratiquement impossible de retrouver les facteurs lorsque le nombre dépasse quelques centaines de chiffres.

On ne sait pas aujourd'hui si le problème de la factorisation est difficile par nature, ou si nous sommes seulement ignorants d'algorithmes efficaces pour le résoudre. En d'autres termes, la sécurité du RSA ne repose sur aucune preuve formelle, et un des grands défis mathématiques du 21^e siècle est de prouver ou d'infirmer cette sécurité.

Le modèle de calcul pour évaluer la difficulté des problèmes est celui de la *Machine de Turing*¹¹⁷, modèle théorique de calculabilité établi par le mathématicien Alan Turing en 1936, modèle dont nos ordinateurs actuels sont des réalisations effectives.

Mais il existe un autre modèle de calcul reposant sur les propriétés des particules élémentaires de la matière : le calcul quantique¹¹⁸. Au niveau microscopique, les particules ont des propriétés d'intrication et de superposition d'état qui ont conduit les chercheurs à concevoir une machine, pour l'instant sans existence réelle, pouvant virtuellement réaliser un nombre exponentiel de calculs simultanément en associant plusieurs particules intriquées. Ce modèle reste pour l'instant théorique, car on ne sait pas aujourd'hui réaliser de dispositif comportant plus d'une dizaine de particules, ce qui limite considérablement la portée pratique.

Mais si ces machines venaient à être construites, elles pourraient implémenter un algorithme efficace de factorisation des entiers rendant obsolète les principaux systèmes cryptographiques en usage aujourd'hui sur Internet¹¹⁹.

Un pan entier de la recherche actuelle en cryptographie est, sous le nom de *Cryptographie Post-Quantique*¹²⁰, l'élaboration de protocoles de sécurité résistant à l'apparition du calculateur quantique.

5.4 - La cryptographie quantique

La physique quantique apporte de son côté sa contribution à l'élaboration de protocoles de diffusion de clé secrète¹²¹. Ces protocoles ont pour but de permettre à deux partenaires distants de s'accorder sur une donnée secrète sur laquelle il existe une certitude absolue qu'aucun adversaire quel qu'il soit ne dispose de la moindre information même partielle. Cette certitude repose les lois de la physique et non pas sur la difficulté supposée ou réelle de problème mathématique difficile. Contrairement au calculateur quantique, cette cryptographie est effectivement mise en œuvre et des entreprises proposent d'ores et déjà des équipements reposant sur ces principes.

Le principe de cet échange de clé repose sur l'indivisibilité des particules élémentaires et sur le théorème de non clonage qui interdit de reproduire à l'identique une particule, son observation modifiant (ou créant selon les interprétations) son état. Les particules sont envoyées unes à unes au destinataire, et le protocole assure que toute interception par un adversaire est détectable.

¹¹⁷ https://fr.wikipedia.org/wiki/Machine_de_Turing

¹¹⁸ https://fr.wikipedia.org/wiki/Calculateur_quantique

¹¹⁹ https://fr.wikipedia.org/wiki/Algorithme_de_Shor

¹²⁰ https://fr.wikipedia.org/wiki/Cryptographie_post-quantique

¹²¹ https://fr.wikipedia.org/wiki/Cryptographie_quantique

Cet échange ne fonctionne que sur des transmissions point à point, limitées en distance, impraticable sur un réseau ouvert comme Internet.

De plus, les protocoles nécessitent, pour leur mise en œuvre, deux canaux de communication :

- un canal dit *quantique* sur lequel les particules sont transmises unes-à-unes. Il s'agit pour l'instant dans la plupart des cas de fibres optiques.

- un canal intègre de réconciliation sur lequel les partenaires échangent des données publiques pour s'accorder sur le secret échangé. Ces données peuvent sans inconvénient être connues d'un adversaire mais il est crucial qu'elles ne soient pas modifiées. L'intégrité des données échangées est une hypothèse majeure sur laquelle repose la sécurité du protocole.

Mais les équipements actuels utilisent le même canal physique pour la réconciliation et assurent l'intégrité par des protocoles de cryptographie conventionnelle à clé publique comme la signature RSA. Ce dernier point limite considérablement l'intérêt de ce type d'équipement, présenté comme un gage de sécurité *post quantique*.

VI – Le droit, ses objets, ses évolutions

6.1. Origines et Evolution de la réglementation en cryptologie

6.1.1. Le développement du télégraphe

6.1.1.1. Le télégraphe optique de Chappe

A la fin du dix-huitième siècle et au début du dix-neuvième siècle, la révolution industrielle a multiplié les échanges. Des réseaux de communications se mettent en place et se développent ; chemin de fer, canaux de communication, routes, etc.

Les réseaux de communications suivent ce mouvement. Le télégraphe de Chappe est adopté par la convention après une démonstration de transmission rapide d'information sur une distance de quarante km en 1793. Il s'en suit une première ligne Paris-Lille qui permet de transmettre un message en moins de six heures. Cette ligne sera suivie par d'autres, pour former un réseau qui couvrira la France métropolitaine, et également l'Algérie et la Tunisie. En 1844, le territoire Français comporte 534 tours couvrant un réseau de plus de 5000 km entre les principales agglomérations du territoire, mais également la Tunisie et l'Algérie.

Jusqu'à son ouverture au public en 1851, le télégraphe de Chappe est réservé aux communications gouvernementales. De ce fait, la question des interceptions revêt un caractère particulier. Le seul problème est de protéger les informations gouvernementales du regard indiscret du public.

Pour cela, l'organisation du télégraphe était très hiérarchique, obéissant à une discipline quasi militaire. Au sommet, se trouve l'administration centrale, composée à partir de 1823 de trois administrateurs, un chef et deux adjoints pour quatre bureaux : dépêches, personnel, matériel et comptabilité.

On trouve ensuite les directeurs qui sont à la tête d'une division et qui ont pour tâche de coder, décoder et émettre les dépêches. Ils supervisent l'activité des inspecteurs qui sont attachés à une division et sont responsable d'un tronçon de ligne d'une dizaine de stations. Les stationnaires représentent 90 % du personnel et sont deux par poste pour faire fonctionner le télégraphe. L'un est chargé de l'observation à la lunette alors que l'autre manipule les commandes.

Le message, n'est compréhensible que par le poste émetteur et le poste destinataire. Il reste incompréhensible pour tous les intermédiaires. Le code repose sur un répertoire de 92 pages, sur chaque page, figure 92 lignes qui comportent chacune un mot ou un groupe de mots. Le livre de code est un répertoire tenu secret de $92 \times 92 = 8454$ entrées et n'est détenu que par les directeurs des stations extrêmes.

6.1.1.2. Le télégraphe électrique

Le télégraphe électrique est conçu dès 1832 par plusieurs inventeurs dont Pavel Schilling (1786-1837), diplomate d'origine allemande au service de la Russie.

En 1838, Charles Weastone installe la première ligne de télégraphe électrique en Angleterre entre Londres et Birmingham.

En 1944, l'américain Samuel Morse (1791-1872) crée le code qui porte son nom et réalise une liaison télégraphique entre Baltimore et Washington. Le code Morse, initialement sensible aux erreurs sera amélioré par l'auteur, journaliste, musicien allemand Friedrich Clemens Gerte (1801-1888), pionnier de la télégraphie qui va lui donner en 1850 sa forme définitive.

Une première ligne électrique installée en France en 1845 entre Paris et Rouen, initiant le déclin du télégraphe de Chappe.

En 1851, le premier câble sous-marin est construit entre l'Angleterre et la France. Le premier câble transatlantique sera mis en service en 1866, après environ dix ans de travaux.

L'extension du télégraphe va conduire à de nouvelles exigences de confidentialité. La revue trimestrielle conservatrice *Quarterly Review*, fondée par John Murray, publie un article en 1853, où il y est écrit :

« Des mesures devront être prises pour parer à une sérieuse objection que l'on soulève à propos des communications privées par télégraphe – la violation du secret – car, dans tous les cas, une demi-douzaine de personnes sont amenées à connaître chaque mot adressé par une personne à une autre. Les employés de la Compagnie Anglaise du Télégraphe s'engagent au secret sous serment, mais nous écrivons souvent des choses que nous ne supporterions pas voir lues par d'autres avant nous. C'est encore un grave défaut du télégraphe, et il faut y remédier d'une manière ou d'une autre. »

La taxation des messages au mot conduit à l'utilisation de codes compressifs. Un des premiers codes commerciaux pour cet usage est le code Sittler de 1868. Les mots et les expressions courantes sont rangés dans l'ordre alphabétique. Ils sont numérotés de 0 à 99 sur chaque page. Une dépêche télégraphique est constituée d'une suite de mots de 4 chiffres indiquant le numéro de la page et l'index du mot dans la page selon une convention admise par les deux correspondants. Ce type de code a autant une fonction compressive que de chiffrement.

La réglementation évolue pour suivre ce besoin. La loi du 13 juin 1866 accorde en France au public la faculté de correspondre en chiffres sur le territoire français. La convention de Saint-Pétersbourg du 10 au 22 juillet 1875 permet l'emploi d'une communication chiffrée pour les communications télégraphiques internationales.

6.1.2. Depuis la deuxième guerre mondiale

Au cours de la deuxième guerre mondiale, la technologie a été un facteur déterminant de la victoire. La guerre a été autant une guerre technologique qu'une guerre du champ de bataille. Les Allemands ont développés les premiers avions à réaction, et les premiers missiles V1 et V2. Les Alliés ont développé des techniques particulières de calcul balistique assisté par un calculateur analogique, ont contré le chiffrement des messages allemands, en particulier entre les sous-marins pour mettre en échec le blocus de l'atlantique imposé à l'Angleterre. L'équipe de Bletchley Park, forte de quelques dix mille personnes a développé les premiers calculateurs aux fins de cryptanalyse.

Conscients de l'importance du secret des communications, une liaison téléphonique chiffrée très sécurisée a été conçue pour sécuriser les échanges entre le président Roosevelt et le premier ministre Churchill. Ce projet ultra secret, appelé SIGSALY, ou CYPHONY ONE (Cyphering Telephony), n'a révélé qu'en 1975. Il a été mis au point sous l'égide du Signal Corp, organisation militaire des transmissions américaines, par les Bell Labs, laboratoire de recherche privé industriel. Des personnalités scientifiques comme Claude Shannon, Alan Turing et William Friedman, y ont participé. Le premier prototype a été expérimenté en novembre 1941, lors d'une liaison transatlantique entre l'Angleterre et les Etats-Unis. Le projet était opérationnel en août 1942.

Les travaux scientifiques menés pour l'effort de guerre pendant la deuxième guerre mondiale ont fortement structuré la recherche scientifique aux Etats-Unis, celle-ci était durablement structurée sur trois piliers que sont l'Armée, l'Industrie et l'Université.

En raison du rôle crucial de la cryptologie dans la victoire des Alliés, à partir de 1945, dans les pays occidentaux, les moyens de chiffrement sont contrôlés par les états et ont le statut d'arme de guerre de deuxième catégorie, au même titre que les munitions. Toute personne disposant sans autorisation de moyens de chiffrement était passible de sanctions pénales. Le régime mis en place en France était celui de la prohibition. Des dérogations pouvaient être accordées au cas par cas étaient accordées par les gouvernements.

Un décret de 1986 a assoupli les conditions d'attribution de ces dérogations pour les applications commerciales.

Avec le développement du réseau Internet, et en particulier celui du commerce en ligne, cette position devenait de moins en moins tenable.

Dans la loi de réglementation des télécommunications du 29 décembre 1990, seuls les moyens de chiffrement destinés aux armées sont considérés comme des armes. Les autres sont déclassifiés, mais toujours soumis à une autorisation d'utilisation.

La réglementation française en matière de cryptologie, édictée par le Service Central pour la Sécurité des Systèmes d'Information (SCSSI, ancêtre de l'ANSSI, dépendant du premier ministre) stipulait :

Si les nouvelles technologies de l'information et de la communication permettent des gains considérables en efficacité et en productivité pour les personnes et les entreprises honnêtes, elles profitent également aux organisations criminelles ou terroristes. Dans le cadre de la protection des personnes et des biens, de la sécurité intérieure et de la défense nationale, l'État doit mettre en place des mesures nécessaires pour éviter que ces technologies ne facilitent, en toute impunité et en toute discrétion, le développement d'actions ou de trafics illégaux (petite et grande délinquance, terrorisme, mafia, pédophilie, blanchiment, fraudes financières, espionnage industriel, ...).

Cette réglementation est le signe d'une tension au sein de l'État entre les tenants d'un contrôle et ceux d'une libéralisation pour favoriser le développement de l'économie numérique.

Plusieurs tentatives ont été mises en place pour concilier ces points de tensions. Il s'agissait de promouvoir les communications sécurisées pour assurer la confiance dans les nouvelles technologies numériques émergentes, tout en donnant aux Etats les moyens de contrôle des communications qui lui permettent d'assurer sa mission de sécurité. Pendant une décennie, la bataille entre les tenants du maintien du contrôle et ceux de la libéralisation s'est centrée autour du problème de la taille des clés. Les états étaient prêts à concéder l'usage d'une cryptographie libre à condition que les clés utilisées ne dépassent pas 40 symboles binaires, c'est-à-dire une taille accessible par recherche exhaustive aux services gouvernementaux. Mais assez rapidement, cette taille étaient également accessible à des organisations privées. Une autre solution a du être mise en œuvre. Les pays occidentaux ont été traversés par des tensions similaires. On examine ci-après deux cas d'école : les États-Unis et la France.

6.1.2.1. Aux États-Unis

Le mouvement de libéralisation de la cryptologie a commencé à la fin des années 1970 avec l'appel d'offre du NIST pour un chiffrement standard (DES, *Data Encryption Standard*) pour les besoins du chiffrement civil. L'agence de sécurité NSA a imposé une taille de clés de 56 symboles binaires, inaccessible en pratique au décryptement par recherche exhaustive sauf pour les grandes institutions gouvernementales disposant de moyens de calcul puissant. La sécurité était assurée pour les entreprises et les citoyens, mais l'État pouvait quand même accéder aux contenus.

Avec le développement de la puissance de calcul accessible au plus grand nombre, une taille de clé de 56 symboles binaires devenait trop faible pour assurer une sécurité acceptable. Les différences de moyens de calcul entre l'industrie et les organisations gouvernementales ne pouvaient plus suffire.

La communauté cryptographique estimait qu'une taille de clé de 80 symboles binaires était la plus petite possible pour assurer une sécurité acceptable.

Les Etats-Unis ont tenté d'imposer la mise en écrou des clés de chiffrement (*Key escrow*). Il s'agit d'un mécanisme dans lequel les clés nécessaires pour déchiffrer les cryptogrammes sont accessibles aux instances gouvernementales en cas de besoin. Ce mécanisme de séquestre des clés a été matérialisé dans un composant, le *Clipper Chip*, qui était un circuit intégré développé et promu par la NSA américaine, et destiné à être implémenté dans les équipements de chiffrement. Ce composant obligeait les utilisateurs à remettre leurs clés en dépôt aux instances gouvernementales afin que les organismes chargés d'appliquer la loi (CIA, FBI) puissent avoir un total accès au trafic à des fins d'interception, de surveillance et de renseignement. Le développement de cette puce a été largement controversée et abandonné en 1996.

6.1.2.2. En France : les tiers de confiance

Dans le but d'assurer une cryptographie forte tout en évitant que les dispositifs cryptographiques ne puissent « être détourné de leur objectif pour restreindre les prérogatives de l'État en lui interdisant d'exercer en totalité sa souveraineté » tout en reconnaissant que « le premier enjeu lié au développement de la société de l'information est celui de la protection de la vie privée, c'est aussi celui qui restera le plus important pour assurer la confiance de notre société dans le numérique », la législation française s'est orienté vers un système de tiers de confiance. L'usage de la cryptologie était soumis à déclaration préalable, avec obligation de déposer les clés chez un tiers de confiance librement choisi. Ces tiers de confiance étaient des sociétés privées indépendantes chargées de fournir et de stocker les clés utilisés par les utilisateurs pour leurs communications privées, a priori sans limitation de taille. Ces clés restaient confinées chez le tiers de confiance jusqu'à ce qu'une décision de justice n'impose de les communiquer à des fins d'enquête.

Le principe était d'utiliser une cryptographie forte, inaccessible à quiconque, tout en permettant, dans certaines circonstances prévues par la loi, aux services de l'État d'avoir accès aux communications.

A l'opposé, les milieux d'affaire faisaient pression pour libéraliser la cryptologie afin de susciter la confiance dans les technologies numériques de communications naissantes et de développer le commerce électronique.

Ces derniers ont eu gain de cause, puisque la « loi pour la confiance dans l'économie numérique » du 21 juin 2004 inscrit dans son article 30 que :

« l'usage des moyens de cryptologie est libre »

Ce n'est pourtant pas la fin de l'histoire. Malgré un usage annoncé comme libre dans la plupart des pays occidentaux Les États n'ont pas renoncé au contrôle de la cryptologie. L'arrangement de Wassenaar (<http://www.wassenaar.org/>) sur les technologies à double usage civil et militaire inclut la cryptologie et oblige les pays exportateurs à un certain contrôle.

6.2. Les arrangements de Wassenaar

Au niveau européen l'exportation des technologies duales a fait l'objet de redéfinition de ses conditions d'application au cours de ces derniers mois (2016). Une modification est apparue nécessaire, dans le cadre des arrangements de Wassenaar, suite aux révélations par WikiLeaks en 2011 des pratiques commerciales d'entreprises européennes, ayant vendu des solutions à des régimes autoritaires. C'est donc des printemps arabes et de l'action des lanceurs d'alerte qu'est née l'expression de ce besoin d'évolution réglementaire. En 2011 et 2012 les embargos européen concernant l'exportation d'armes vers l'Iran et la Syrie ont intégré les technologies de cybersurveillance.

Les arrangements de Wassenaar ont été modifiés en 2012 et 2013, intégrant à la liste des technologies duales devant faire l'objet de contrôle, quelques technologies de surveillance :

équipements de brouillage, équipements d'interception des télécommunications mobiles, systèmes de surveillance des réseaux IP, logiciels d'intrusion. Puis ces équipements et systèmes furent intégrés à la liste européenne en décembre 2014.

Les révélations concernant les pratiques de la NSA par E. Snowden ont-elles conforté l'institution européenne dans sa détermination à réguler, contrôler, et opposer la notion de sécurité des individus à la sécurité nationale par exemple, mais aussi à la liberté de commerce ?

Il semblerait que le contournement des restrictions à l'exportation touchant les outils d'interception soit chose relativement aisée : il est possible d'acquérir sur internet du matériel d'interception tactique par exemple¹²².

La liste des technologies duales est disponible sur le site officiel wassenaar.org¹²³.

Fait	Date	Commentaire
Création du CoCom (<i>Coordinating Committee for Multilateral Export Controls</i>)	1949	Contrôler le marché de technologies pouvant être duales (usage civil et militaire). Un groupe réduit d'Etats règle les exportations de ces technologies. On est au sortir de la seconde guerre mondiale. Les Etats-Unis dominent ce système de régulation.
Dissolution du CoCom	1996	
Arrangements de Wassenaar	Mai 1996	Objectifs : régulation, contrôle des exportations, enjeux de sécurité et défense nationale, protection des citoyens, constitution d'un marché, défense des intérêts économiques, militaires, technologiques des Etats
Le Royaume-Uni propose d'ajouter des technologies de surveillance intrusives à la liste des « armes » de l'arrangement de Wassenaar ¹²⁴	2013	

Rappelons qu'il revient à chaque Etat d'appliquer, selon son appréciation, le contrôle des exportations d'armes conventionnelles et technologies à double usage. L'effectivité des arrangements de Wassenaar dépend donc de l'application qu'en décident les Etats¹²⁵. Les différences nationales créent donc des marges de manœuvre pour les uns, des contraintes pour les autres.

¹²² Pierluigi Paganini, An investigation conducted by The Motherboard demonstrates that is quite easy to buy Surveillance Equipment avoiding export restrictions, 19 janvier 2016, <http://securityaffairs.co/wordpress/43711/security/tactical-surveillance-technology-investigation.html>

¹²³ <http://www.wassenaar.org/wp-content/uploads/2016/12/WA-LIST-16-1-2016-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf>

¹²⁴ <https://insidersurveillance.com/off-rails-wassenaar-arrangement-on-export-controls-for-surveillance/>

¹²⁵ <http://convention-s.fr/decryptages/larrangement-de-wassenaar-et-la-reglementation-des-technologies-de-surveillance-a-usage-double/>

VII - Conclusion

Ce premier rapport du projet UTIC s'est attaché à esquisser un panorama des diverses questions d'ordre technique et technologique que soulève l'interception des communications électroniques, comme moyen de la cybersurveillance.

Le premier point qu'il nous semblait important de traiter était celui de la terminologie. Plusieurs termes et expressions sont employés dans les discours traitant des interceptions et de la surveillance, concurrents ou complémentaires, parfois synonymes. Quelques rappels de définitions permettent de préciser ces concepts clefs.

Nous avons tenu à rappeler les liens qui unissent le présent et le passé, au travers d'une lecture historique des sciences et des techniques pouvant être associées aux pratiques de l'interception des communications. Nous avons également esquissé une lecture juridique, en avançant quelques pistes que la suite du projet devra approfondir, notamment celle du poids des Arrangements de Wassenaar dans la régulation internationale des technologies d'interception qui peuvent être considérées comme des technologies duales. Ces incursions dans des approches qui ne sont plus seules considérations techniques (comprendre la manière dont est structuré l'Internet, comment fonctionne le chiffrement, les outils qui sont à disposition de l'interception), sont nécessaires. Car on ne saurait traiter des capacités d'interception en réduisant l'approche à la seule question technologique. Pour nombre d'entre elles, l'interception des communications à des fins de cybersurveillance étatique, n'est d'ailleurs souvent qu'une application parmi d'autres. Ce sont des contextes socio-politiques, économiques, juridiques, qui en conditionnent les utilisations et les développements. Nous devons donc considérer les diverses dimensions de la question « capacitaire ». Les capacités techniques, technologiques, peuvent être décrites du point de vue de leur fonctionnement, de ce qu'elles permettent de faire, de leur puissance (par exemple de calcul, de traitement, de stockage...) ou de leur dimensionnement (opposer les capacités des data center de l'Utah, aux Etats-Unis, à celles de pays plus modestes). Les capacités d'interception et plus largement de cybersurveillance, dépendent également du niveau de la R&D, de maîtrise et d'avance par rapport à d'autres, dans des domaines aussi divers que les mathématiques, l'informatique, les sciences de l'information, etc. Les capacités sont également humaines (quelles expertises peuvent être mobilisées). Elles sont bien évidemment aussi industrielles, privées, publiques, civiles, militaires : qui fait quoi, qui produit, qui utilise, achète, possède, décide, quelles sont les interactions (une sociologie des organisations serait ici pertinente, tout comme une approche économique). Le projet UTIC, dans le prolongement de ce premier livrable, pourra ainsi analyser de manière approfondie les conditions juridiques qui déterminent les développements et les marchés des capacités technologiques, ainsi que les capacités d'action (comment les moyens techniques à disposition sont exploités). L'interaction entre plusieurs cadres juridiques, nationaux, internationaux (droit européen versus Arrangements de Wassenaar par exemple) pourra constituer l'un des axes de travail.

La géopolitique des câbles et des data centers apparaît par ailleurs primordiale. Les quelques données introduites dans le rapport concernant l'étendue et l'infrastructure câblée du réseau mondial, imposent une recherche plus approfondie, afin de tenter de cartographier les relations entre câbles sous-marins et terrestres, d'identifier les acteurs clefs du développement de ces infrastructures (Etats, entreprises), afin de répondre à des questions telles que : qui possède quoi ? Où ? Et quel pouvoir cela donne-t-il aux Etats en matière d'interception ?

Une étude de la structuration des industries et des marchés s'avèrera également indispensable. En effet, notre sentiment est que les industriels pèsent sur les normes juridiques (en matière de régulation des technologies duales notamment) et que le marché des solutions d'interception est mondial, sans véritables frontières. Ces industries se rencontrent, se croisent sur des salons internationaux, sont en concurrence, mais savent coopérer lorsque cela est nécessaire pour répondre à des appels d'offre, afin d'intégrer leurs solutions. L'interception semble ainsi nécessiter plusieurs formes de coopération, aucun acteur ne paraissant être en mesure de posséder toutes les briques nécessaires à sa mise en œuvre et à sa maîtrise de bout en bout : coopération public-privé, civil-militaire, inter-entreprises (intégrer des solutions complémentaires), interétatique (des agences

de renseignement échangent, partagent leurs compétences), à l'échelle nationale ou internationale. De ces relations nécessaires découlera une dépendance respective, y compris des Etats les uns envers les autres. Ces modalités multiples d'organisation et la diversité des acteurs (recherche universitaire, industrie, agences de renseignement, etc.) constituent le cadre dans lequel les capacités technologiques viennent servir des usages et des objectifs particuliers. Au regard de ces analyses, il sera alors question des rapports de force qui configurent la scène internationale.

VIII – Bibliographie complémentaire

8.1. Ouvrages, articles (par ordre chronologique)

- Pontaut J.M. (1978), *Les secrets des écoutes téléphoniques*, Paris
- Beltran A., Griset P. (1990), *Histoire des techniques aux XIX^e et XX^e siècles*, Paris, Colin, « Coursus », 190 p.
- Branch Ph. (2003), *Lawful interception of the internet*, Australian Journal of Emerging Technologies and Society, n°1, 14 pages, <http://www.ibap.com.au/Resources/Interception%20of%20the%20Internet%20by%20Dr%20Philip%20Branch.pdf>
- Ehrlich T. (2004), *Case study on lawful intercept*, Harvard Law School, 11 novembre, 23 pages, https://cyber.harvard.edu/globaleconomy/lawful_intercept.pdf
- Gellis C.R. (2006), "Copysense and sensibility – how the wiretap act forbids universities from using P2P monitoring tools", *B.U.J.SCI. & TECH.L.*, Vol 12, n°2, 34 pages, http://www.bu.edu/law/journals-archive/scitech/volume122/documents/gellis_web_000.pdf
- Cross T. (2010), "Exploiting lawful intercept to wiretap the Internet", BlackHat Conference, 41 pages, https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-Lawfull-Intercept-slides.pdf
- Chow K.P. (2011), "Internet surveillance technologies in Hong Kong", University of Hong Kong, 37 pages, <http://www.lawtech.hk/wp-content/uploads/2011/01/Internet-Surveillance-Session-III-KP-Chow-1545-1610.pdf>
- Stevens A. (2011), "Surveillance policies, practices and technologies in Israel and the occupied territories: assessing the security state", novembre, 23 pages, http://www.sscqueens.org/sites/default/files/2011-11-Stevens-WPIV_0.pdf
- Wagner B. (2012), "Exporting censorship and surveillance technology", 19 pages, https://www.hivos.org/sites/default/files/exporting_censorship_and_surveillance_technology_by_ben_wagner.pdf
- Fuchs Ch. (2012), « Implications of deep packet inspection (DPI) Internet surveillance for society », Department of Informatics and Media, Uppsala University, Research Paper n°1, juillet, 127 pages, <http://fuchs.uti.at/wp-content/uploads/DPI.pdf>
- Garcia L.F. (2013), "Internet surveillance technologies in Mexico", Juin, 26 pages, http://media.espora.org/mgoblin_media/media_entries/1173/INTERNEWS_Internet_surveillance_in_Mexico.pdf
- Schlehahn E. (et alt.) (2013), « Report on surveillance technology and privacy enhancing design », juin, 99 pages, projet européen Surprise, <http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf>
- Xynou M. (2014), « The surveillance industry in India », Researc paper, 48 pages, <http://cis-india.org/internet-governance/blog/surveillance-industry-india.pdf>

8.2. Autres rapports et études d'organisations et institutions (par ordre chronologique)

- Secretary of State for the Home Department, *Interception of Communications in the United Kingdom. A consultation Paper*, Juin 1999, 34 pages, <http://www.cyber-rights.org/interception/ioca.pdf>
- Interception of communications in the United Kingdom. A consultation paper, Presented to Parliament by the Secretary of State for the Home Department, by Command of her Majesty, juin 1999, Royaume-Uni, 34 pages, <http://www.cyber-rights.org/interception/ioca.pdf>
- European Parliament, "Development of surveillance technology and risk of abuse of economic information", Document de travail pour le panel STOA, Décembre 1999, 135 pages,

http://blog.m0le.net/streisand.me/autoblogs/refletsinfo_5efe27982e35e61b381760cd425aa17aa8d2dc43/media/89ad23a4.DG-4-JOIN_ET28199929168184_EN.pdf

- The interception of communications act, 15 mars 2002, Jamaïque, 26 pages, http://www.unodc.org/tldb/pdf/Jamaica_Interception_of_Communications_Act.pdf
- University of Oxford , « Legal opinion on Intercept Communication”, Faculty of Law, The Justice Project, janvier, 45 pages, 2006, <http://www.cyber-rights.org/interception/ioca.pdf>
- Interception of communications and surveillance ordinance, Hong Kong, 2006, 39 pages, [http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/DDA393C36B7FE4BA482575EF001FD1A4/\\$FILE/CAP_589_e_b5.pdf](http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/DDA393C36B7FE4BA482575EF001FD1A4/$FILE/CAP_589_e_b5.pdf)
- Annual Reports to the Chief Executive by the Commissioner on Interception of Communications and Surveillance, Hong Kong, rapports des années 2006 à 2014 accessibles à partir du lien <http://www.info.gov.hk/info/sciocs/en/reports.htm>
-
- Interception of communications. Code of practice, Home Office, Londres, 2007, 42 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/513668/interception-comms-code-practice.pdf
- Interception of communications act, Zimbabwe, 2007, 12 pages, http://www.vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf
- ITU, “Technical aspects of lawful interception”, mai 2008, 12 pages, http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf
- The Interception of communications bill, 2010, 34 pages, <http://www.ttparliament.org/legislations/b2010h22.pdf>
- Interception of communications act, Trinidad and Tobago, 2010, version amendée de 2012, 34 pages, http://www.oas.org/juridico/PDFs/cyb_tto_int2010.pdf
- “Monitoring internet communications”, mai 2013, Postnote, Houses of Parliament, UK, 4 pages, <http://researchbriefings.files.parliament.uk/documents/POST-PN-436/POST-PN-436.pdf>
- Ultimaco, *Lawful interception in the digital age: vital elements of an effective solution*, 26 pages, 2014, https://lms.utimaco.com/fileadmin/assets/brochures_datasheets_whitepapers/UTIMACO_LIMS_WHITEPAPER_EN.pdf
- “Gaining total visibility for lawful interception”, juillet 2014, IXIA White Paper, 8 pages, <http://researchbriefings.files.parliament.uk/documents/POST-PN-436/POST-PN-436.pdf>
- FIDH, “Surveillance technologies ‘made in Europe’. Regulation Needed to prevent human rights abuses », France, 40 pages, 2014 https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe-1-2.pdf
- Cause (2014), “A critical opportunity: bringing surveillance technologies within the E.U. Dual-use regulation”, 26 pages, <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>
- Interception of communications. Code of practice, Londres, 2015, 34 pages, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf
- Report of the interception of communications commissioner, mars 2015, Presented to Parliament pursuant to Section 58(6) of the Regulation of Investigatory Powers Act 2000, Londres, 104 pages, [http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20\(Web\).pdf](http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf)