Surveillance «profonde» sur internet

LIBERTÉS PUBLIQUES • *La Libye, l'Egypte ou la Tunisie ont pu surveiller les communications des citoyens grâce à du matériel de sociétés occidentales, qui pouvaient tester leurs techniques à grande échelle.*

LE MONDE diplomatique

ANTOINE CHAMPAGNE*

Le Caire, 30 mars 2011. Hosni Moubarak aurait utilisé les produits de la firme Narus, qui compte comme client la NSA, l'agence de sécurité nationale américaine, à l'origine du projet Echelon. KEYSTONE

Visitant, après la chute de Tripoli, un centre dédié à l'écoute de la population, la journaliste du *Wall Street Journal* Margaret Coker a pu constater que tout y était surveillé: le réseau internet, les téléphones mobiles GSM et les connexions (internet et téléphone) par satellite. Dans des dossiers figuraient, entre autres choses, les courriels ou des extraits de conversations en ligne d'opposants au régime de Mouammar Kadhafi. Sur les murs du centre, des affichettes de l'entreprise qui avait mis en place cette installation: Amesys, une filiale de la société française Bull[1]. *Le Canard enchaîné* révèlera par la suite que la direction du renseignement militaire (DRM) avait été sollicitée pour aider à la formation des «surveillants» libyens[2].

En Syrie, c'est du matériel américain qui permet au régime de Bachar El-Assad de censurer internet et de récupérer comme bon lui semble les identifiants et mots de passe des citoyens, afin d'accéder à leurs messageries électroniques ou à leurs pages sur les réseaux sociaux Facebook et Twitter. Un outil particulièrement efficace pour reconstituer les interactions d'un opposant avec des appuis intérieurs ou extérieurs.

Les technologies employées portent le doux nom de Deep Packet Inspection (DPI, en français «inspection en profondeur des paquets»). Lorsqu'on envoie un courriel, des dizaines de machines se relaient pour l'acheminer jusqu'au destinataire. Se contentant de consulter l'adresse de destination, elles n'en regardent pas le contenu et le transmettent directement au voisin. De proche en proche, le courrier parvient à destination. Comme l'explique Jonathan Zittrain, spécialiste du droit d'internet, «c'est un peu comme dans une soirée avec des gens polis. Si vous êtes trop loin du bar et qu'il y a trop de monde pour s'en approcher, vous demandez à votre voisin de vous faire parvenir une bière. Il demande alors à son voisin qui est, lui, un peu plus proche du bar, etc. En fin de compte, votre demande parvient jusqu'au bar et la bière revient par le même chemin. Comme tout le monde est poli, personne n'a bu dans votre verre pendant l'opération.[3]»

Avec le DPI, c'est une autre vision de l'internet qui se met en place. Moins polie. Que diriez-vous si votre voisin analysait votre commande et commençait par vous faire la morale? Ou s'il décidait de changer le contenu de votre verre, pour y verser de l'eau, ou un euphorisant plus fort? C'est ce que permettent les techniques de DPI: lire le contenu des conversations, les modifier, les envoyer à quelqu'un d'autre…

Sur ce marché, la société Amesys n'est pas isolée. Qosmos, autre société française, vient de se faire épingler par Bloomberg. L'agence de presse américaine a en effet révélé qu'elle avait fourni des sondes DPI à un consortium chargé d'équiper la Syrie sur le même modèle que la Libye de Kadhafi[4]. En Chine, les technologies de DPI sont au cœur du grand pare-feu qui permet au gouvernement de censurer les conversations et d'espionner les citoyens.

De fait, comme le montre la récente livraison, par le site WikiLeaks, de nombreux documents internes de ces sociétés, la surveillance des réseaux de communication est «une nouvelle industrie secrète recouvrant vingt-cinq pays. (…) Dans les histoires d'espionnage traditionnelles, les agences de sécurité comme le MI5 britannique mettent sur écoute le téléphone d'une ou deux personnalités intéressantes. Au cours des dix dernières années, les systèmes de surveillance massive et indiscriminée sont devenus la norme.[5]» Un peu plus tôt, le *Wall Street Journal* avait publié plus de deux cents documents marketing émanant de trente-six sociétés proposant aux autorités antiterroristes américaines divers outils de surveillance et de piratage[6].

Aux Etats-Unis, le DPI a connu son heure de gloire en mai 2006: Mark Klein, ancien technicien de AT&T (gros fournisseur d'accès internet américain), sort alors du silence. Il dénonce l'installation, chez son ancien employeur, et donc au cœur du réseau internet américain, de produits de la société Narus. Maître d'œuvre, la fameuse National Security Agency (NSA), inventrice dans les années 1980-1990 du projet Echelon[7]. La devise de Narus: «See Clearly. Act Swiftly» («Voir clair. Agir vite»). Créé en 1997, cet éditeur de technologie DPI, avec ses cent cinquante employés, a levé 30 millions de dollars en 2006, et a été racheté par Boeing en 2010. Ses produits auraient été installés en Egypte à l'époque de Hosni Moubarak[8].

La plupart des flux d'informations sont échangés en clair

Parmi les flux d'informations qui transitent par internet, les opérateurs de télécommunications voient passer du Web, des courriers électroniques, des discussions en temps réel, des échanges vocaux, de la vidéo, des discussions asynchrones, des données brutes, etc. La plupart de ces flux sont échangés en clair, sans chiffrement cryptographique. Il est donc aisé, pour le pirate du dimanche comme pour les services de sécurité étatiques, de les placer sur écoute.

Mais certains acteurs privés trouvent aussi un intérêt dans ces technologies. Les opérateurs de télécommunications comme Free, SFR ou Orange commencent à se plaindre de voir passer sur leur réseau des masses de données en provenance d'acteurs qui ne payent pas pour ce transport. Par exemple, les fournisseurs d'accès à internet (FAI) trouvent désagréable de payer pour les vidéos en provenance de YouTube, qu'ils sont obligés de servir à leurs abonnés. D'où l'idée de facturer un supplément à l'émetteur des données ou à l'utilisateur final, ou encore de ralentir sélectivement certains flux, pour en privilégier d'autres. Mais, pour cela, il est indispensable de mesurer avec précision ce qui passe dans les tuyaux.

De même, les opérateurs de téléphonie mobile ont décidé, pour essayer de limiter leurs coûts d'infrastructure, de ne fournir à leurs usagers qu'un accès bridé à internet. Ils interdisent donc aux utilisateurs de téléphones «intelligents» de procéder à des échanges de fichiers en pair-à-pair ou d'utiliser des outils de communication vocale ou vidéo tels que Skype.

Là encore, c'est le DPI qui leur permet de pratiquer la surveillance et la gestion des flux, d'allouer une «bande passante» supérieure à certains services (par exemple, ceux qu'ils éditent…). En contradiction avec la notion de «neutralité du réseau», qui affirme que le rôle du fournisseur d'accès est de faire transiter sans discrimination toutes les données demandées.

Appliqué à la navigation sur le Web, le DPI permet de garder une trace de tout ce que vous y faites. Les professionnels du marketing se frottent les mains et rêvent d'exploiter ces données. Orange a d'ailleurs tout récemment lancé une offre «Orange préférence», reposant sur du DPI, qui se propose, avec l'accord de l'abonné, d'analyser les sites Web qu'il visite pour lui proposer ensuite des offres commerciales ultraciblée. De quoi permettre aux FAI de devenir aussi rentables que Facebook et Google. A condition que ces programmes de fidélisation-surveillance attirent des abonnés; mais il suffira de clamer que les données sont anonymisées pour en faire un produit parfaitement commercialisable.

Le lecteur curieux pourra consulter la page «Data Privacy» du site de GFK, un groupe international de recherche en marketing actionnaire de Qosmos: s'il évoque, banalement, les cookies des navigateurs internet, il omet d'expliquer qu'il utilise aussi, pour «tracer» les visiteurs des sites internet, une technologie DPI, prétendument «anonymisée» par une recette connue de lui seul. GFK est présent dans plus de cent cinquante pays, et pas uniquement de grandes démocraties…

Le DPI attire aussi les sociétés d'ayants droit et les détenteurs de copyright qui souhaitent lutter contre les échanges de fichiers «illégaux» sur les réseaux en pair-à-pair ou les sites de téléchargement direct, du type Megaupload, récemment fermé par la justice américaine. Savoir précisément quel internaute tente de télécharger tel ou tel film ou fichier musical, et réussir à lui en bloquer l'accès, ne peut se faire qu'avec une infrastructure de surveillance «profonde» et répartie sur l'ensemble des points d'échange de données que sont les FAI.

Les professionnels du marketing rêvent d'exploiter ces données

Un autre marché naturel du DPI concerne la surveillance légale. La police a parfois besoin d'écouter ce que fait un particulier, dans le cadre d'une instruction judiciaire, sous le contrôle d'un juge et, en France, d'une «commission de contrôle des interceptions de sécurité». Cependant, il s'agit d'un marché de niche, ne concernant qu'une très faible partie de la population. A moins de tabler sur une nouvelle augmentation fulgurante des budgets consacrés à l'antiterrorisme, il paraît sage pour les entreprises du secteur de rechercher d'autres débouchés commerciaux.

C'est là qu'interviennent les gouvernements d'Etats policiers, qui souhaitent écouter toute la population. Grâce à ces pays, les logiciels de surveillance sont testés en grandeur nature. La Tunisie de Zine El-Abidine Ben Ali bénéficiait ainsi de rabais pour des systèmes où subsistaient encore des bugs. Quant à Amesys, la Libye a sans conteste été une expérimentation grandeur nature de ce que peut faire (ou pas) son logiciel Eagle[9]. Alcatel opère de même en Birmanie[10]. De fil en aiguille, l'exploitation des données récoltées par le DPI facilite les arrestations. La torture fait le reste, les bourreaux reprenant les bonnes vieilles techniques qu'ils connaissent et qui donnent des résultats.

Probablement intrigué par la présence massive d'entreprises européennes sur ce type de marchés, le parlement européen a passé une résolution destinée à proscrire la vente à l'étranger de systèmes de surveillance des appels téléphoniques et des textos, ou fournissant une surveillance ciblée d'internet, s'ils sont utilisés pour contrevenir aux principes démocratiques, bafouer les droits humains ou la liberté d'expression[11]. Le 1er décembre 2011, le Conseil de l'Union européenne, durcissant les mesures restrictives à l'égard du régime syrien, a ainsi interdit «les exportations d'équipements et de logiciels destinés à la surveillance d'internet et des communications téléphoniques.

Mais la fourniture de produits d'écoute globale reste mal encadrée sur le plan juridique. Il reste aisé pour les producteurs de passer entre les mailles du filet. D'autant que les législations sont diverses. Les autorisations données par le gouvernement ne sont pas publiées. Et les logiciels de ce genre ne sont pas considérés stricto sensu comme des armes. I

*Journaliste, Reflets.info

[1] Paul Sonne et Margaret Coker, «Firms aided Libyan spies», *The Wall Street Journal*, New york, 30 août 2011.
[2] «Des experts des services secrets français ont aidé Kadhafi à espionner les Libyens», 7 septembre 2011, et «Secret militaire sur le soutien à Kadhafi», 12 octobre 2011, *Le Canard enchaîné*, Paris.
[3] Jonathan Zittrain, «The web as random acts of kindness», conférence TED, juillet 2009, www.ted.com
[4] «Syria crackdowm gets Italy firm's aid with US-Europe spy gear», Bloomberg, 3 novembre 2011.
[5] WikiLeaks, «The spy files», 1er décembre 2011.
[6] Jennifer Valentino-Devries, Julia Angwin et Steve Stecklow, «Document trove exposes surveillance methods», *The Wall Street Journal*, 19 novembre 2011.
[7] Lire Philippe Rivière, «Le système Echelon», *Manière de voir*, n° 46, «Révolution dans la communication», juillet-août 1999.
[8] Timothy Karr, «One US corporation's role in Egypt's brutal carckdown», The Huffington Post, 28 janvier 2011.
[9] *Cf.* le dossier Amesys sur le site Reflets.info.
[10] Diane Lisarelli et Géraldine de Margerie, «Comment Alcatel se connecte à la junte birmane», *Les Inrockuptibles*, Paris, 26 mars 2010.
[11] «Le parlement européen interdit la ventre de technologies de surveillance aux dictatures», 11 octobre 2011, www.fhimt.com

Paru dans *Le Monde diplomatique* de janvier 2012.