COMMENT L'AMÉRIQUE

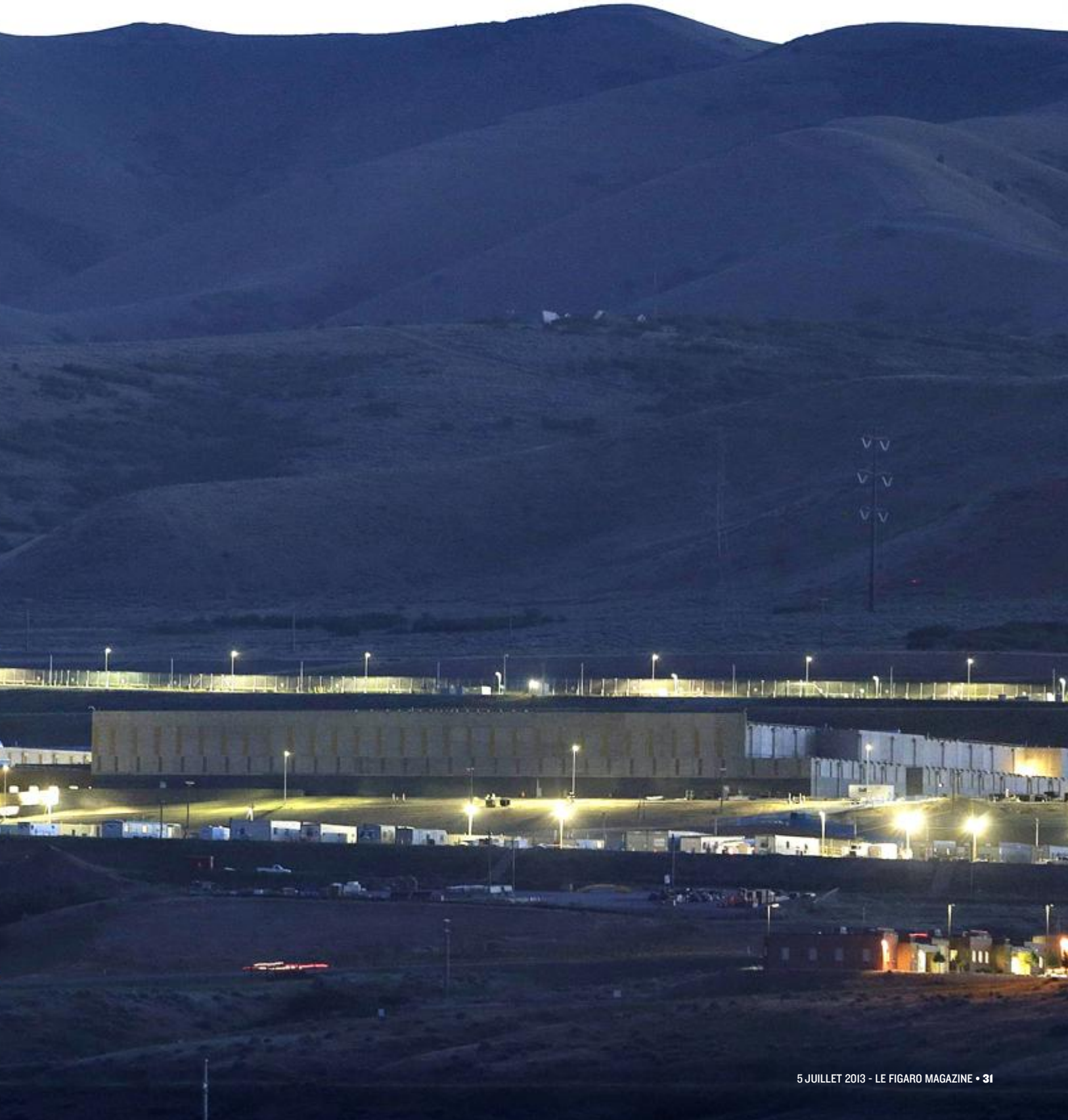
EN COUVERTURE *En révélant l'existence d'un programme nommé Prism, l'analyste Edward Snowden a provoqué un coup de tonnerre. Ce sésame ouvre toutes les portes d'internet à la puissante National Security Agency (NSA). Mais sa panoplie et ses capacités d'espionnage vont bien au-delà. Révélations sur la pieuvre américaine.*

PAR JEAN-MARC GONIN ET VINCENT NOUZILLE

Le centre de stockage de données de Bluffdale (Utah). Prévu pour ouvrir en septembre prochain, il va devenir le « coffre-fort » de la NSA. L'agence américaine aura la capacité d'y stocker 100 ans d'informations véhiculées par internet. Pour cette installation remplie de high-tech dernier cri, l'agence fédérale aurait investi 2 milliards de dollars.

RICK BOWMER/AP/SIPA

NOUS ESPIONNE



FIGARO PLAY EN VIDÉO : « Comment protéger ses données personnelles sur internet ? Parole d'un avocat d'expert. »

Le serveur de Facebook installé à Prineville, dans l'Oregon. La société a démenti avec véhémence avoir accordé à la NSA un accès direct à ses bases de données. Elle n'a fait que répondre à des requêtes de la justice.

ALAN BRANDT/AP/SIPA

Le web. La toile. Cette image d'un réseau tissé tout autour de la planète où, chaque seconde, circulent des milliards d'informations – textes, photos, sons, vidéos – peut aussi ressembler à un filet, une nasse, voire un chalut aux capacités infinies. La révélation de l'existence du système Prism par l'analyste américain Edward Snowden, un système mis au point et utilisé par la National Security Agency (NSA), en donne l'impression. En se branchant directement sur les principaux câbles, en puisant continuellement dans les informations qui y circulent, en se ménageant un accès aux serveurs des acteurs majeurs d'internet, l'agence de renseignement américaine s'est dotée d'un passe-partout auquel rien ne résiste. Comme si les agents de la NSA pouvaient à tout moment, et comme bon leur semble, perquisitionner dans la correspondance, la sphère personnelle, voire privée, de chaque internaute sans mandat officiel, et sans que l'intéressé s'en aperçoive. Pour un espion,

ANDREW GOBERT/EPA/MAXPPP

Edward Snowden, l'analyste à la source du scandale, affirme avoir agi au nom de la protection des libertés.

Prism est un rêve devenu réalité, le nec plus ultra du renseignement, le paradis de la surveillance. D'un coup, grâce à une porte dérobée, on peut fouiller, lire, copier des informations de première main que l'internaute a lui-même écrites, envoyées, stockées. Pour la liberté de chacun, en revanche, Prism est un cauchemar. Aucun d'entre nous, surtout s'il n'est pas citoyen des Etats-Unis, n'est à l'abri de ce « cyber-regard » inquisiteur.

Si Edward Snowden, 30 ans, employé depuis trois mois à la société Booz Allen Hamilton, basée à Hawaï, a tiré le signal d'alarme, c'est au nom de la liberté. Ce virtuose de l'informatique était chargé par son employeur, lui-même sous-traitant de la NSA, d'exploiter et d'analyser les informations siphonnées par l'agence de renseignements sur le réseau internet. Il n'a pas supporté. Et il a provoqué une affaire d'Etat qui embarrasse Barack Obama.

En prenant la fuite, d'abord à Hongkong, avant de poursuivre sa cavale par Moscou, le jeune homme a emporté avec lui quatre ordinateurs portables où il a stocké des données sur les activités de la NSA dont il a eu connaissance. Quand il nous apprend via la presse – les quotidiens *Washington Post* et *The Guardian*, l'hebdomadaire allemand *Der Spiegel* – que des ambassades de France, d'Italie ou de Grèce, ou des représentations de l'Union européenne, voire le siège de la Commission à Bruxelles, ont été mis sur écoute par l'espionnage américain, l'affaire ne sur-

La NSA a le pouvoir de fouiller dans la vie de chacun d'entre nous

prend guère. Les coups fourrés entre alliés ne datent pas d'hier *(voir page 40)*. En revanche, ses révélations sur Prism retentissent comme un coup de tonnerre. Le document majeur constitue une présentation de type Power Point (une série de visuels expliquant le fonctionnement du système espion) destinée aux analystes. Selon cet élément ultraconfidentiel, la NSA disposerait d'accès aux serveurs des plus grands noms de l'internet : Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube, Apple... Excusez du peu. Rares sont les internautes dans le monde qui n'ont pas au moins un lien avec un de ces fournisseurs d'accès ou de messagerie. En d'autres termes, la NSA a le pouvoir de fouiller dans la vie de chacun d'entre nous.

La loi garantit l'immunité aux sociétés qui coopèrent

Pour pratiquer cette quête sans entrave, la NSA s'appuie sur des législations adoptées en 2007 et 2008 sous George W. Bush dans la foulée des lois antiterroristes postérieures aux attentats du 11 septembre 2001. Une législation reconduite par Obama en décembre 2012. En garantissant une immunité aux sociétés privées qui coopéreraient avec les agences de renseignement, donc en les abritant des poursuites judiciaires, les autorités fédérales américaines ont circonvenu les géants du web. Selon le document révélé par Edward Snowden, Microsoft a été le premier à franchir le pas il y a six ans. Les autres ont suivi. Le cadre légal est suffisamment flou pour permettre aux agences de renseignement de ratisser le plus large possible : il leur suffirait d'évoquer les soupçons de terrorisme et d'espionnage pour justifier la collecte d'informations. Selon les textes, la Foreign Intelligence Surveillance Court (cour de surveillance du renseignement étranger) , qui est un tribunal ad hoc et ultrasecret, chargé de veiller à l'application de la loi sur l'espionnage étranger (Fisa), doit donner un feu vert à chaque demande. En fait, les analystes de la NSA ne se heurtent qu'à un obstacle majeur : les citoyens américains. La cour veille aux droits des citoyens américains, ce qui oblige les agents de la NSA à effectuer un signalement chaque fois qu'ils tombent sur un compatriote. Les autres nationalités n'ont pas ce privilège.

DPA/MAXPPP

A Hanovre (Allemagne), des manifestants ont défilé contre les agissements de la NSA. L'Allemagne est une des premières cibles de l'agence américaine.

Dès que les documents sur Prism ont été révélés, les sociétés privées en cause ont publié une rafale de communiqués. Tous ont nié avec la plus grande fermeté avoir connaissance du système Prism. Tous ont contesté avoir concédé à la NSA un accès direct à leurs serveurs. Et chacun de déclarer qu'il se conformait à la loi et ne divulguait aux agences fédérales que les informations réclamées par un mandat légal ou une assignation de la justice. Pour démontrer leur bonne foi, les stars d'internet ont dévoilé combien de demandes d'information ont été satisfaites à la demande de la NSA. Entre le 1er juillet et le 31 décembre 2012, Facebook a déclaré avoir reçu entre 9 000 et 10 000 requêtes de l'agence fédérale portant sur 18 000 à 19 000 comptes. Durant la même période, Microsoft dit avoir reçu entre 6 000 et 7 000 mandats concernant entre 31 000 et 32 000 comptes clients. De son côté Yahoo ! a fait part de 12 000 à 13 000 demandes entre le 1er janvier et le 31 mai dernier. Apple, lui, a signalé entre 4 000 et 5 000 requêtes portant sur 9 000 à 10 000 comptes et appareils. Google n'a pas voulu se plier à cet exercice. Ses dirigeants entendent intégrer ces chiffres à son « rapport de transparence » publié chaque année.

Derrière la levée de boucliers des acteurs d'internet se cache l'avenir même de la Silicon Valley *(voir encadré page 37)*. La crainte est d'autant plus forte que Snowden a fait des émules. Dans le *G2 Bulletin*, une lettre spécialisée sur le renseignement publiée aux Etats-Unis, on apprend que tous les logiciels Windows depuis la version 95 comportent deux clés de cryptage ; la première se nomme KEY, la seconde NSAKEY. Un curieux acronyme qui laisse deviner que l'agence fédérale dispose d'un formidable passe-partout pour accéder à tous les PC équipés de ce système d'exploitation.

Ce n'est pas le seul moyen de la NSA pour surveiller tout ce qui se passe. Grâce à ses propres *crawlers*, des robots d'in- ...

LA PIEUVRE

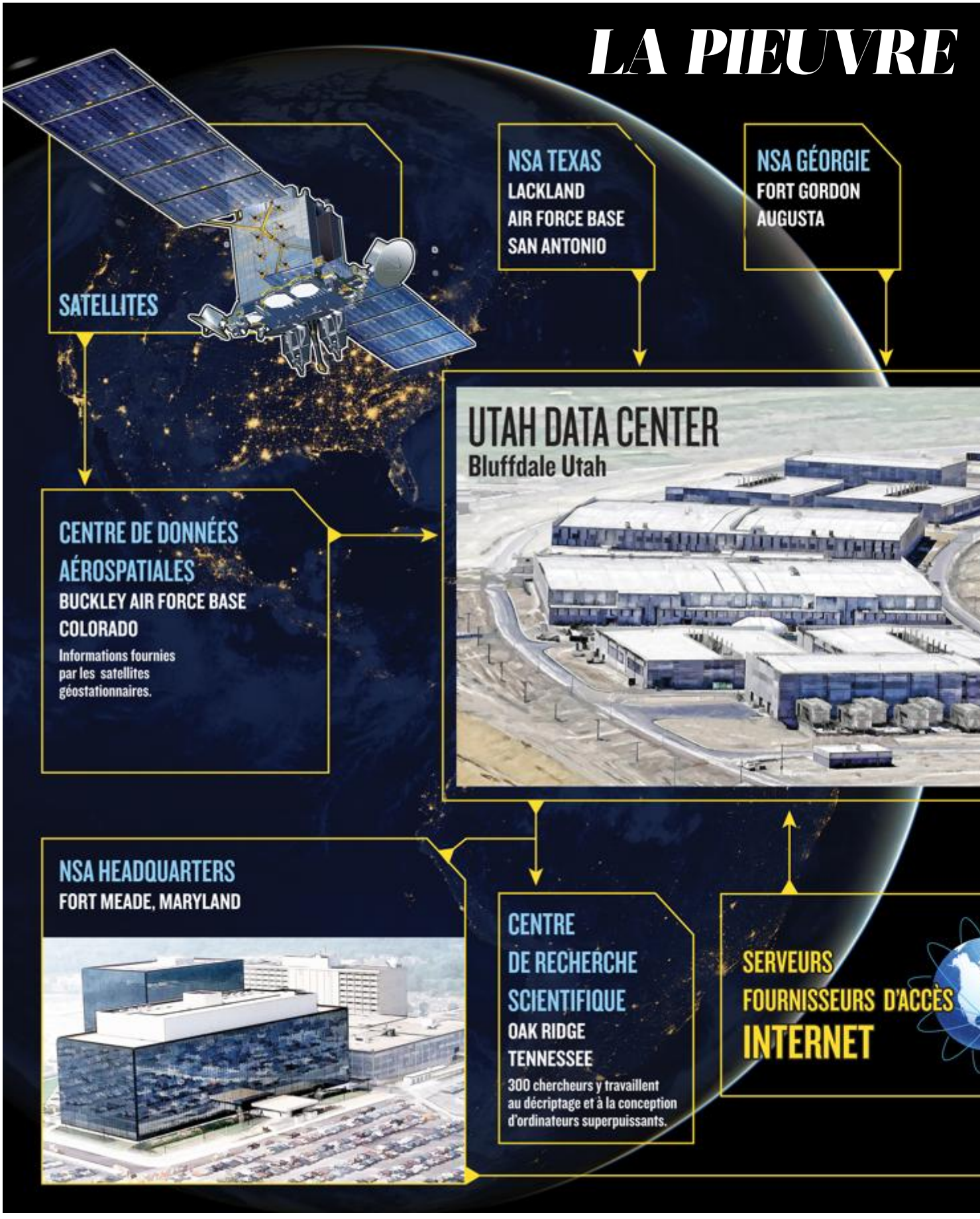
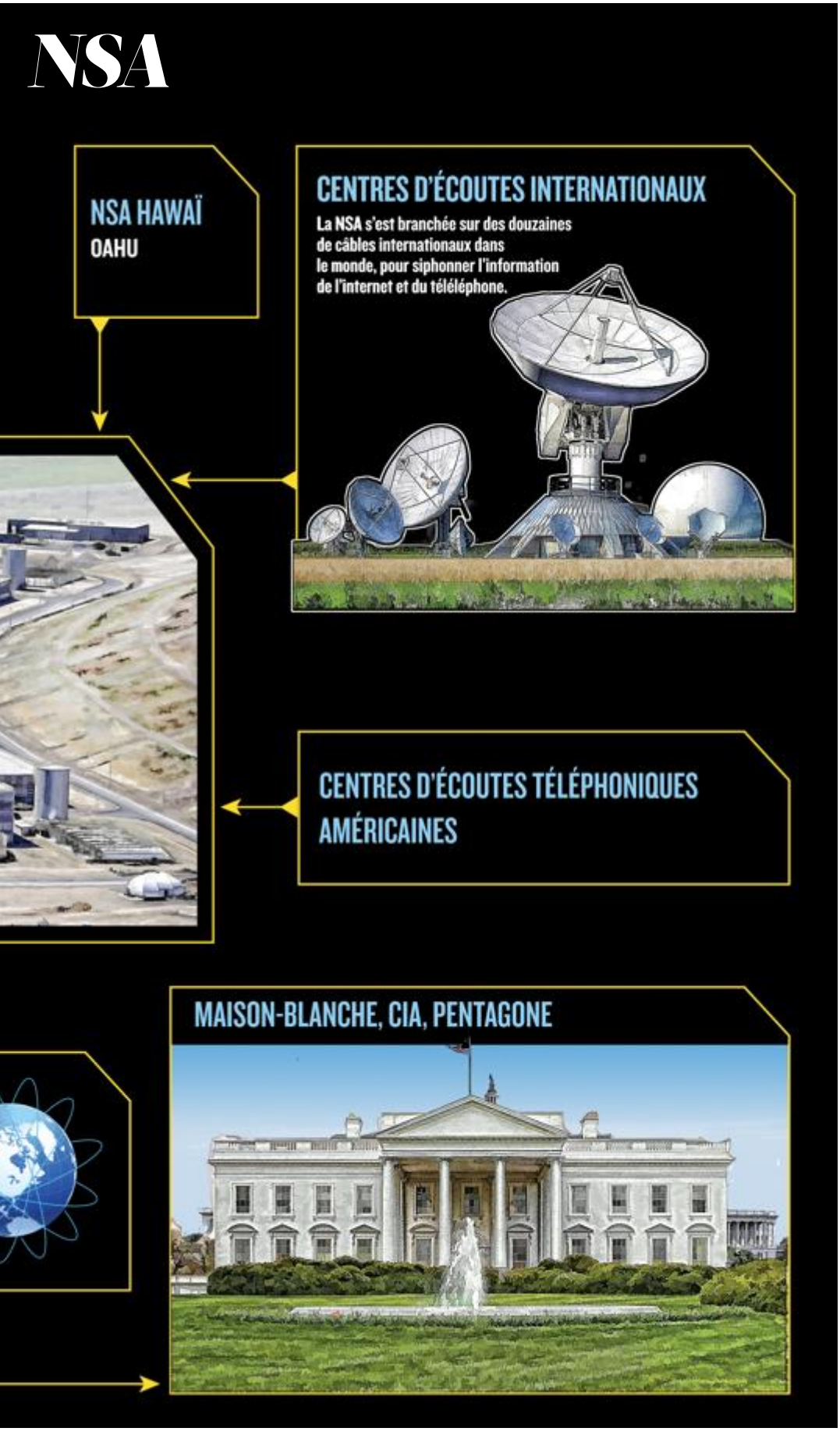
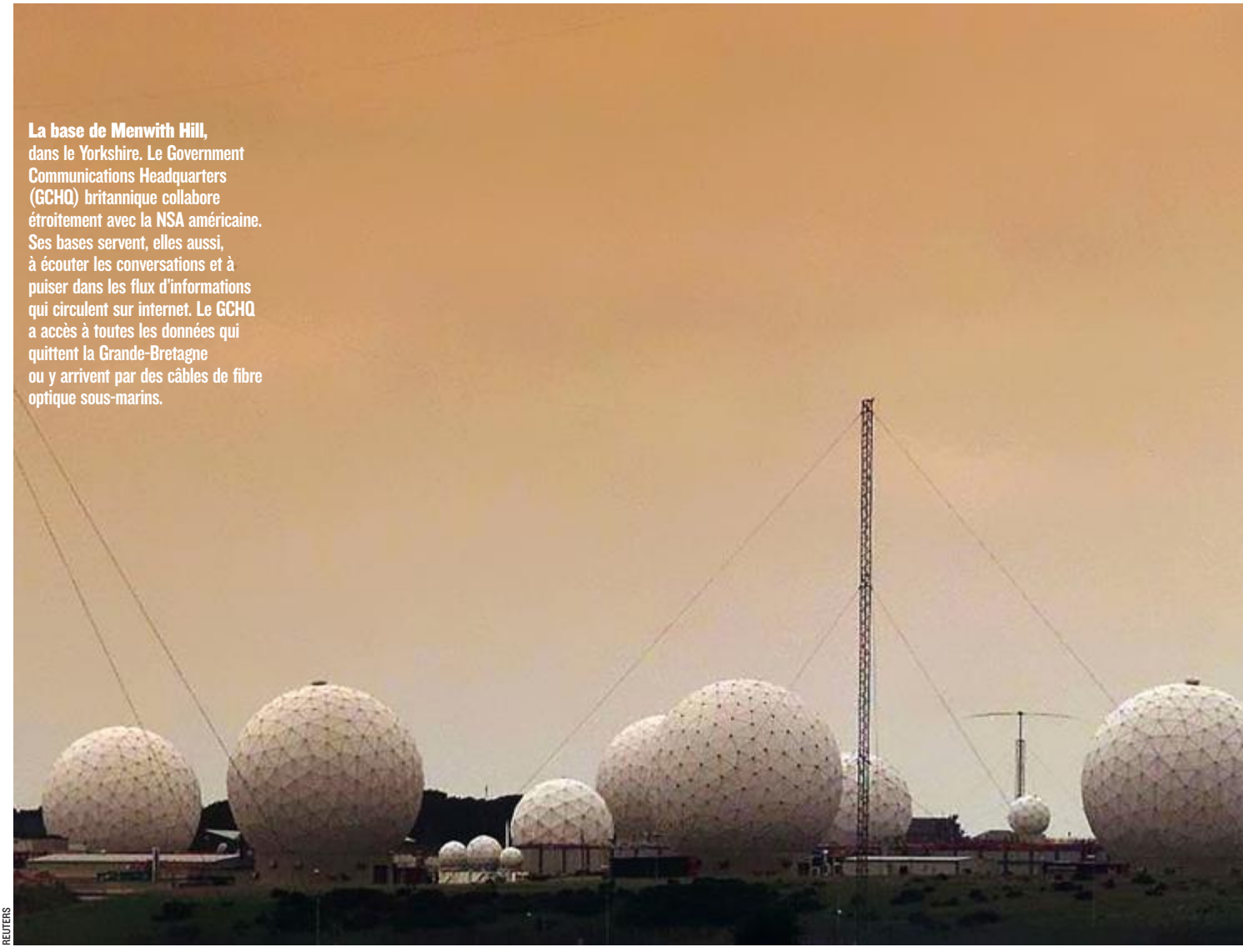


ILLUSTRATION ANDRÉ DE CHASTENET

NSA



Le Data Center (centre de stockage de données) de la National Security Agency (NSA) ouvrira dans deux mois à Bluffdale, dans l'Utah. Cet ensemble ultrasecret d'une superficie de 9,3 ha aurait la capacité de stocker un siècle de communications internet dans le monde. Sa construction aura coûté 2 milliards de dollars. Bluffdale sera le nouveau cœur de la NSA, qui dispose d'un budget annuel classé secret défense, mais estimé entre 8 et 10 milliards de dollars. Cette agence collecte des données grâce à une série d'installations. Quatre satellites géostationnaires captent les fréquences hertziennes (téléphones, talkies-walkies, radars…) traitées par le centre de Buckley (Colorado). Plusieurs bases aux Etats-Unis analysent les interceptions : celles en provenance d'Europe, du Moyen-Orient et d'Afrique du Nord sont traitées à Augusta (Géorgie), celles d'Amérique latine à San Antonio (Texas), et celles d'Asie à Hawaï. Plus d'une dizaine de stations d'écoute sont dédiées aux communications téléphoniques américaines. A l'étranger, la NSA dispose d'une douzaine de branchements sur les câbles de communication. Le système Prism complète le dispositif en offrant des accès aux serveurs des principaux opérateurs d'internet et de téléphonie mobile. L'analyse des quelque 100 milliards d'informations pêchées chaque mois dans le monde sont transmises au QG de Fort Meade, près de Washington. La NSA se taille la part du lion dans les briefings quotidiens de renseignements fournis au président Obama. En 2012, les données obtenues grâce à Prism auraient représenté 1 477 informations délivrées à la Maison-Blanche, soit un rapport sur sept.



La base de Menwith Hill, dans le Yorkshire. Le Government Communications Headquarters (GCHQ) britannique collabore étroitement avec la NSA américaine. Ses bases servent, elles aussi, à écouter les conversations et à puiser dans les flux d'informations qui circulent sur internet. Le GCHQ a accès à toutes les données qui quittent la Grande-Bretagne ou y arrivent par des câbles de fibre optique sous-marins.

REUTERS

Internautes traqués selon leurs déviances

••• dexation et de recherche, l'agence a la capacité de procéder à des recoupements très fins. *« L'analyse des métadonnées permet de cibler certains numéros, des flux de messages vers des suspects, des profils types de personnes dangereuses »*, explique un vétéran de la lutte antiterroriste de la CIA, très admiratif de ces nouveaux outils techniques. Mais cet usage justifié masque d'autres objectifs. Les robots peuvent s'avérer très utiles pour repérer des « cibles » potentielles d'actions clandestines d'une autre nature. Les données recueillies sur les recherches menées via Google permettent, par exemple, de remonter dans le temps, de manière indéfinie, traquant ainsi le moindre comportement « anormal ». La visite, même occasionnelle, de sites pornographiques, pédophiles, violents, racistes ou extrémistes est détectable. Les internautes peuvent ainsi être classés et « tracés » selon leur degré de déviance. Même les échanges de mails avec une maîtresse cachée, des messages ambigus sur Facebook ou un penchant masqué pour les forums gays servent d'élément déclencheur. *« Les services américains risquent d'utiliser ces infos pour faire pression sur un internaute qui les intéresse, par exemple, le cadre d'un grand groupe bancaire ou aéronautique qu'ils veulent espionner*, raconte un ancien expert de la DGSE. *L'un des secrets du renseignement, c'est justement de pouvoir connaître les vulnérabilités des cibles et de savoir, le jour venu, s'en servir. »* Naguère, le KGB était réputé maître dans l'art de piéger des cibles, avec l'argent, le sexe ou l'alcool. Aujourd'hui, les Américains sont capables de faire de même avec ce qu'ils savent des petites faiblesses de tout internaute. *« Ce qui relève, a priori, de la vie privée peut servir, demain, dans la compétition économique »*, renchérit Franck Bulinge, professeur de management de l'information à l'ISC Paris et auteur du livre *De l'espionnage au renseignement. La France à l'âge de l'information* (Vuibert).

Clinton met l'accent sur le renseignement économique

Car la NSA ne se contente pas de *« lutter contre le terrorisme »*. *« C'est une excuse pour accroître son pouvoir »*, explique James Bamford, historien et auteur de plusieurs ouvrages de référence sur la NSA. Car la notion de « sécurité nationale », qui a

Le général Keith B. Alexander, directeur de la NSA et patron du Cybercommand. Surnommé « l'empereur Alexandre », il explique à ses visiteurs qu'il veut tout savoir sur tout. Outre le renseignement, il est en charge de la stratégie en matière de guerre cybernétique.

NSA

donné son nom à l'agence, est élastique. D'abord centrée sur l'URSS durant la guerre froide, la NSA a rapidement étendu ses grandes oreilles tous azimuts. Les stations d'écoute de son réseau d'interceptions Echelon, fruit de l'alliance des services de renseignement de cinq pays anglo-saxons (Etats-Unis, Canada, Royaume-Uni, Australie, Nouvelle-Zélande) drainent des milliards d'informations chaque jour vers le quartier général de Fort Meade, dans le Maryland. Dès le milieu des années 90, le président Bill Clinton et son bras droit Al Gore ont donné comme consigne aux services secrets, NSA et CIA, de s'orienter vers le renseignement économique, afin de conquérir tous les marchés. Et de ne pas rater la révolution numérique. *« Nous savions dès cette époque qu'ils s'étaient branchés sur les réseaux internet, à partir de trois centres d'interception, situés sur la côte Est, à Chicago et en Californie »*, raconte un ancien expert du ...

LES GÉANTS DE L'INTERNET INQUIETS

Peur sur la Silicon Valley

Dans la Silicon Valley, l'affaire Prism a sonné le tocsin. Soudain, les plus grands noms de l'internet, les entreprises stars des dernières décennies, les Microsoft, Apple, Google, Facebook, Yahoo et consorts se sont retrouvés confrontés au soupçon de fournir les données de leurs clients à des agences de renseignement américain. Pis, selon Edward Snowden, les espions disposeraient d'un accès direct à leurs serveurs. Une à une, les sociétés mises en cause ont opposé de fermes démentis aux allégations publiées par le *Washington Post* et le *Guardian*. Leurs porte-parole ont divulgué les chiffres des demandes d'information transmises par la NSA et dûment approuvées par un mandat d'un tribunal spécial. Tandis qu'Edward Snowden a promis d'en dire plus sur le sujet, la Silicon Valley retient son souffle. Deux dangers guettent les géants d'internet. D'un côté, ils craignent que leurs clients – surtout les non-Américains – perdent confiance et ferment leurs comptes pour éviter que leurs données privées soient transmises à l'espionnage américain. De l'autre, ils redoutent que l'affaire Snowden provoque un renforcement de la sécurisation des données et de la protection de la sphère personnelle. Si tel était le cas, le trésor que représente la revente des fichiers à d'autres sociétés s'évanouirait pour de bon. Que seraient Facebook, Google, Skype sans les précieuses données sur les utilisateurs collectées jour après jour ? Ils deviendraient de simples forums dépourvus de valeur marchande. J.-M. G.

FIGARO PLAY

Défendre les intérêts américains en oubliant les alliés

NSA

Le siège de la NSA à Fort Meade (Maryland), là où aboutissent les milliers d'analyses produites par les fonctionnaires et les sous-traitants de l'agence fédérale. Avec un budget supérieur à 8 milliards de dollars, la NSA est devenue le poids lourd du renseignement américain.

••• secrétariat général à la Défense nationale. *« Depuis la chute du mur de Berlin, en réalité, la NSA se concentre à 80 % sur le renseignement économique »,* poursuit un haut gradé français, qui se souvient d'avoir été reçu plusieurs fois à Fort Meade. *« Chaque fois, nous étions accueillis très poliment par le grand patron de l'époque, le général Michael Hayden, mais ce dernier restait peu bavard sur ses programmes ! »*

Son successeur, le général Keith Alexander, nommé en 2005 par le président Bush, a repris le flambeau. *« Ce n'est pas un dictateur, ni le Dr Folamour,* confie un ancien dirigeant de la DGSE qui a pu le rencontrer. *Mais il m'a dit plusieurs fois, sur le ton de la plaisanterie qu'il voulait tout intercepter sur tout, partout. Je ne savais comment le prendre, mais je crois, en fait, que c'était de la franchise ! »* Et, en bon militaire, Alexander défend strictement les intérêts des Etats-Unis, sans trop se soucier de ses alliés.

Pour mener sa guerre numérique, le grand patron de la NSA ne recule devant aucune démesure. Outre ses dizaines de stations d'écoute, ses 40 000 employés, ses centaines de superordinateurs Cray, son centre géant de stockage de données, dont le chantier de 2 milliard de dollars est en cours de finition à Bluffdale, dans l'Utah, il dispose d'outils complémentaires qui lui donnent une vue d'ensemble des mouvements financiers planétaires. D'après plusieurs sources concordantes, la NSA a été l'un des parrains officieux du système de virements bancaires Swift, né en 1973 et basé à Bruxelles, devenu une sorte de passage obligé pour les mouvements de fonds des plus grandes banques et courtiers mondiaux, puisqu'il voit passer plus de 20 millions de transactions par jour. Les députés européens Verts ont d'ailleurs réclamé en début de semaine le blocage de l'accès aux données bancaires de ce système pour faire pression sur le gouvernement américain. La NSA appuie également discrètement les programmes de The Advocacy Group, une association parapublique de lobbying qui soutient les entreprises américaines partout dans le monde.

Par ailleurs, son puissant réseau de sous-traitants constitue une armée supplémentaire de cerveaux et un moyen de collecter d'autres renseignements. Près de 500 000 de leurs salariés sont accrédités « Top secret », avec des accès aux programmes de renseignement. Parmi eux, on trouve naturellement des équipes des plus grands groupes du complexe militaro-industriel, de Boeing à Lockheed-Martin, de Raytheon à Endgame. Mais aussi quelques milliers d'experts et scientifiques de SAIC, une discrète société d'ingénierie basée près de San Diego, en Californie, ainsi que des milliers de consultants de la firme Booz Allen & Hamilton, chez qui travaillait Edward Snowden. Le concepteur de la cyberstratégie de cette société n'est autre que Mike McConnell, l'un des anciens patrons de la NSA. La nébuleuse NSA comprend également des sociétés informatiques amies comme IBM, grand spécialiste du *cloud computing,* qui permet de délocaliser ses données, ou Intel, premier fabricant de microprocesseurs, et sa filiale de sécurité McAfee. Spécialisée dans la cyberdéfense et les antivirus, cette dernière reconnaît qu'elle travaille, comme Intel, *« avec la NSA »,* mais *« ne veut pas en dire plus sur la nature de ses relations avec l'agence »,* même si elle dément tout accès direct à ses serveurs. En réalité, elle participe au dispositif de cyberguerre mis en place depuis quelques années par la NSA et les autorités américaines.

Une cyber-attaque le jour de la fête nationale

En 2009, McAfee a ainsi rédigé un rapport alarmiste sur les cybermenaces, établi par Paul Kurtz, ancien membre du Conseil de sécurité nationale et du Comité pour la sécurité intérieure sous les présidences de Bill Clinton et George W. Bush. Car, le 4 juillet 2009, jour de la fête de l'Indépendance américaine, une série d'attaques informatiques provenant de 50 000 ordinateurs a pris pour cible la Maison-Blanche, le ministère de la Sécurité intérieure, celui du Trésor et de la Défense, la

NSA, ainsi que la Bourse de New York, le Nasdaq ou les sites d'Amazon et Yahoo ! Quelques jours après, les sites web du gouvernement sud-coréen étaient visés, tout comme des communications de l'armée américaine dans le pays. Les attaques étaient attribuées à la Corée du Nord et rappelaient d'amers souvenirs aux vétérans de la guerre de Corée. *« C'est justement parce que les services de renseignement américains n'avaient pas anticipé l'attaque nord-coréenne de 1950 que la NSA a été créée en 1952 »*, explique Philippe Hayez, coordonnateur des études sur le renseignement à Sciences-Po Paris.

Dès la mi-2009, le secrétaire à la Défense Robert Gates a annoncé la création d'un « cybercommandement » rattaché directement à celui des armées. Sa mission : défendre les réseaux stratégiques américains, qu'ils soient privés ou publics. A sa tête, le général Alexander, désormais surnommé « l'empereur Alexandre », qui ajoute cette casquette à celle de patron de la NSA, laquelle était déjà autorisée, selon des documents déclassifiés obtenus par l'association National Security Archive, à mener des attaques cybernétiques. *« Mais ce cumul de fonction à la NSA et au cyber-commandement, tout à fait inhabituel, donne au général Alexander un pouvoir considérable »*, commente James Bamford. Dans ce contexte de paranoïa aiguë, où la collecte des informations est une arme, tous les coups sont permis, y compris l'attaque. Le général Alexander dispose à sa guise d'une armée de plusieurs milliers de hackers, capables de pénétrer les sites officiels de pays alliés comme la France, de pirater les universités chinoises, de propager des virus comme Stuxnet dans les centres nucléaires iraniens, ou de bloquer des communications. *« On ne voit que la partie visible de l'iceberg et il n'y a aucune règle, ni aucune législation puisque internet est une zone de non-droit international »*, précise un expert en sécurité. *« De la même façon que les Etats-Unis se sont abstraits de certaines contraintes juridiques dans la lutte contre le terrorisme, que ce soit à Guantanamo ou via leurs drones tueurs, ils peuvent s'autoriser tout type d'attaque et d'intrusion informatique au nom de leur sécurité nationale »*, regrette Franck Bulinge. Nous voilà prévenus : plus rien n'échappe à la pieuvre NSA. Et elle n'a pas que des intentions amicales.

■ JEAN MARC GONIN ET VINCENT NOUZILLE

DAMIEN BANCAL, EXPERT EN SÉCURITÉ INFORMATIQUE, EXPLIQUE UN CAS CONCRET

Que peuvent-ils savoir sur vous ?

Notre exemple est cadre dans une banque française. Appelons-le Marc-Antoine. Il passe le plus clair de son temps entre téléphone, internet, courriers électroniques et smartphone dernier cri. Il a entendu parler du système d'espionnage Prism, mais il n'y a pas prêté plus attention que ça : il ne se sent pas concerné. Pourtant, Marc-Antoine ne le sait pas encore, mais sa vie numérique finira tôt ou tard par attirer les regards d'un malveillant du numérique. D'abord parce qu'il est le maillon d'une chaîne qui pourrait servir à collecter des informations concernant son travail, ses clients ; ensuite, parce qu'il peut servir de « rebond » à un espionnage économique orchestré par un concurrent.

Marc-Antoine, comme des millions d'internautes, utilise Gmail, l'outil de communication du géant Google. Sur le papier, l'outil est parfait. Intuitif, rapide et consultable partout. Il permet de recevoir et d'envoyer des courriers, de stocker des informations. Bref, un système web pratique... et hébergé aux Etats-Unis. La situation géographique compte : Marc-Antoine est basé à Lille, mais ses données transitent par des serveurs situés en Californie. Des machines qui analysent les contenus des courriels pour... la publicité. Des annonces ciblées par AdWords, le système de Google qui affiche des annonces très précises en fonction du contenu des courriels que vous envoyez/recevez. Pour réussir ce tour de passe-passe, les robots Google, tout comme ceux de son concurrent direct Microsoft, analysent les messages. Autant dire qu'un service d'espionnage peut faire de même et regrouper les informations interceptées via d'autres bases de données.

De plus, le Patriot Act, loi fédérale américaine votée après le 11 Septembre pour lutter contre le terrorisme, autorise FBI, CIA, NSA à écouter, à regarder et à lire ce qui transite par le sol américain. Sans oublier que Marc-Antoine, lors d'un récent voyage aux Etats-Unis, a rempli une fiche Esta avec une série d'informations privées et réglé les formalités avec une carte bancaire.

Les « fuites » d'informations s'exploitent de plus en plus facilement grâce à des outils grand public. Google, encore lui, via son moteur de recherche, permet d'extraire des informations oubliées sur des serveurs, des sites internet. A noter que des sites web tels que le russe Gegereka.com sont encore plus efficaces que l'homologue américain. Des sites totalement légaux qui ne font que référencer ce qui est accessible. Mais revenons à Marc-Antoine. Il ne quitte pas son smartphone, un téléphone dernier cri grâce auquel il navigue sur internet, twitte et converse avec ses amis sur Facebook. Sauf que son mobile l'espionne davantage que dix agents de la CIA réunis. Notre cadre n'a pas pris le temps de lire la notice de son téléphone. A chaque message, il diffuse sa position exacte, au mètre près, grâce au GPS intégré. Il twitte de son domicile, de son bureau... Bref, avec Google Maps et les coordonnées GPS ainsi diffusées, il est même possible de regarder la rue du domicile de notre apprenti geek. En cliquant sur l'onglet satellite de l'option Google, on peut carrément survoler la maison de notre banquier !

Ce fan d'automobile ne sait pas que la télécommande d'activation de sa voiture peut aussi le trahir. Une clé sans contact qui permet, avec un lecteur approprié, de connaître l'identité de l'automobile, son kilométrage, ses récentes utilisations, autant de détails techniques qui régaleraient un agent secret. En 2013, George Orwell ne pourrait plus publier *1984*. Face aux réseaux qui enregistrent les faits et gestes de notre vie quotidienne, son Big Brother est un enfant de chœur. Prism a largement dépassé la fiction. D. B.