De futurs travaux pourraient nous apporter des informations sur des périodes encore plus anciennes de l'histoire de l'Univers. Si nous parvenons à étendre nos observations de l'EBL jusqu'à inclure quelques sources de rayons gamma à plus grand décalage vers le rouge, les astronomes pourraient étudier comment l'Univers a été réionisé au cours du premier milliard d'années après le Big Bang, la lumière ultraviolette des premières étoiles ayant ionisé les atomes neutres de la matière qui composait l'Univers en leur arrachant des électrons. Cet objectif est l'une des principales motivations du prochain télescope international CTA (*Cherenkov telescope array*, « réseau de télescopes Tcherenkov ») en cours de conception, avec des installations dans les hémisphères Nord et Sud, qui seront constitués de différents instruments conçus pour être sensibles aux rayons gamma, des plus basses énergies aux plus hautes.

Par ailleurs, une fois que nous comprendrons et quantifierons mieux l'EBL, nous pourrons soustraire son atténuation des observations de blazars et de sursauts gamma afin de décrire plus complètement la nature de ces objets exotiques eux-mêmes.

En attendant, l'intensité de l'EBL mesurée indirectement par notre technique d'atténuation des rayons gamma est globalement compatible avec l'intensité de l'EBL estimée indépendamment à partir d'observations de galaxies d'époques plus anciennes. Cet accord signifie que la lumière émise par les galaxies aux longueurs d'onde des domaines optique et proche infrarouge semble expliquer les observations de l'EBL par l'intermédiaire de l'atténuation des rayons gamma. Un tel résultat nous conforte dans notre compréhension du fond diffus extragalactique et sur les conclusions que nous en tirons sur l'évolution des galaxies.

## Regarder vers l'avenir

À mesure que nous affinerons nos mesures, l'accord entre les observations directes des galaxies et indirectes à partir des blazars pourrait être renforcé ou, au contraire, montrer des anomalies. Dans un cas, nous pourrons alors fixer des limites sur la présence dans l'Univers de sources de lumière, telle la désintégration d'hypothétiques particules qui se seraient formées dans l'Univers primordial, et dans l'autre cas mettre en évidence de nouveaux phénomènes astrophysiques tels que la désintégration de particules exotiques se convertissant en rayons gamma. Les observations des rayons gamma seront grandement améliorées par la mise en service de CTA, mais c'est toute une nouvelle génération de télescopes spatiaux (le télescope *James Webb*), de télescopes au sol de plus de 30 mètres de diamètre, ainsi que le programme LSST *(Large synoptic survey telescope)* qui permettront de mieux comprendre la formation des galaxies.

Nous connaissons maintenant la réponse au paradoxe d'Olbers : le ciel nocturne n'est pas sombre ; il est rempli de la lueur de toutes les galaxies qui ont existé depuis le commencement de l'Univers, même si cette lueur est difficile à détecter. Et en permanence, des supernovæ explosent, des nuages de gaz luisent et de nouvelles étoiles naissent, ajoutant leur lumière à ce fond omniprésent qui emplit chaque centimètre cube du cosmos. ■

# S'adapter à la CYBERG

Keren Elazari

**Chaque appareil connecté est une cible potentielle pour les cybercriminels. Les gouvernements ne pourront sécuriser le cyberespace que si les particuliers sécurisent leurs propres équipements.**

En termes de cybersécurité, aiment à dire les spécialistes, il existe deux types d'organisations : celles qui ont été touchées et celles qui ne le savent pas encore. Les récents titres de la presse tendent à leur donner raison. Des cybercriminels ont volé les informations des cartes de crédit et les données personnelles de milliers de clients de sociétés telles que les entreprises américaines Target et Home Depot (grande distribution) ou JPMorgan Chase (société de portefeuille). Les chercheurs en sécurité informatique ont découvert des failles fondamentales dans les constituants d'Internet, telle la vulnérabilité Heartbleed dans la bibliothèque de logiciels de cryptographie OpenSSL. Une destruction massive de données a obligé Sony Pictures Entertainment à revenir au papier et au crayon. Des criminels ont accédé aux données de plus de 80 millions de clients de l'entreprise américaine d'assurance maladie Anthem. Et il ne s'agit que des incidents les plus connus.

Dans les années à venir, les cyberattaques vont probablement s'intensifier. Le problème nous concerne tous. Nous sommes tous, d'une façon ou d'une autre, connectés au cyberespace – *via* les téléphones, les ordinateurs portables, les réseaux d'entreprise –, et donc exposés. Le piratage des réseaux, serveurs, ordinateurs personnels et comptes en ligne est devenu une ressource essentielle tant des cybercriminels que des services d'espionnage des États. Votre réseau local d'entreprise, votre PC de jeu deviennent autant d'outils supplémentaires dans l'arsenal des criminels – ou des cyberespions financés par le contribuable. Les ordinateurs compromis servent de tremplin pour l'attaque suivante ou deviennent les maillons d'un «botnet», un réseau malveillant de machines zombies contrôlées et louées à l'heure pour lancer des attaques par déni de service (qui rendent un service indisponible) ou distribuer des spams.

En réponse à de telles menaces, le réflexe des gouvernements consiste à militariser le cyberespace, à essayer de contrôler le monde numérique en s'appuyant sur des agences secrètes et des administrations centralisées. Mais cette approche ne fonctionnera jamais. Elle risque même d'empirer les choses. La cybersécurité est comme un problème de santé publique : seules, les agences de santé

# GUERRE

gouvernementales n'ont pas les moyens d'arrêter la propagation des maladies. Elles ne peuvent remplir leur rôle que si les citoyens remplissent le leur.

## Un cyberespace multiforme

Une difficulté pour protéger le cyberespace est que celui-ci n'est pas une entité unique. Le cyberespace est un vaste ensemble de systèmes interconnectés en perpétuelles mutation et croissance. Pour en prendre la mesure, il faut remonter un demi-siècle plus tôt, aux travaux de Norbert Wiener, professeur de mathématiques à l'Institut de technologie du Massachusetts. En 1948, Wiener a emprunté un terme du grec ancien pour décrire une nouvelle discipline qu'il développait : la cybernétique, ou l'étude du « contrôle et de la communication chez l'animal et la machine ». En grec ancien, *κυβερνήτης* désignait le timonier ou le pilote qui dirigeait et contrôlait les navires en Méditerranée. Par analogie, le cyberespace est l'ensemble des technologies électroniques et numériques interconnectées qui permettent le contrôle et la communication de tous les systèmes sur lesquels repose la vie moderne. Le cyberespace est constitué d'un large éventail de technologies de commande à distance et de communication, allant des pompes à insuline pilotées par radiofréquences aux satellites de géolocalisation GPS.

Le cyberespace n'est pas une eau internationale. Il ne s'agit pas d'un ensemble de territoires que des gouvernements ou des armées pourraient contrôler. La plupart des technologies et réseaux qui constituent le cyberespace sont détenus et entretenus par des multinationales à but lucratif.

Le nombre et la diversité des technologies incluses dans cet espace croissent rapidement. Le fournisseur de matériel réseau Cisco Systems prédit que d'ici 2020, 50 milliards d'appareils seront connectés à Internet, dont, pour une grande part, des dispositifs et systèmes liés à l'industrie, l'armée et l'aérospatiale. Chaque nouveau dispositif qui se connecte au cyberespace est une cible potentielle et les attaquants décèlent vite les maillons les plus faibles des réseaux. Les pirates qui se sont introduits fin 2013 dans les terminaux de points de

### L'ESSENTIEL

- **Les cyberattaques se multiplieront dans les années à venir. Tout utilisateur des technologies modernes est une cible potentielle.**
- **Les nouvelles attaques visent certes les données, mais aussi les objets connectés et les infrastructures matérielles.**
- **Seuls, les gouvernements et l'industrie technologique ne peuvent sécuriser le cyberespace.**
- **Avec l'aide des pirates informatiques et des particuliers, il faut construire un système « immunitaire » distribué.**

vente du distributeur américain Target et ont volé les données de millions de cartes bancaires, par exemple, ont pénétré dans le réseau du détaillant en s'attaquant d'abord à une cible facile : Fazio Mechanical Services, l'entreprise de maintenance frigorifique qui gère les systèmes de chauffage et de réfrigération de Target. Ceux qui, en 2011, ont accédé aux réseaux de l'entreprise américaine de défense Lockheed Martin s'en sont d'abord pris à la compagnie de sécurité RSA, qui fournissait à Lockheed Martin ses jetons d'authentification. RSA elle-même a été compromise parce qu'un employé de sa société mère, EMC, avait ouvert un fichier Excel attaché en pièce jointe à un courriel.

Les « objets » de l'Internet des objets – smartphones, tablettes, animaux marqués d'une puce… –, tous ces éléments auxquels Internet s'étend aujourd'hui, ne sont pas simplement des fenêtres *via* lesquelles les attaquants peuvent s'infiltrer. Ils constituent eux-mêmes des cibles potentielles de sabotage. Dès 2008, des chercheurs en sécurité ont prouvé qu'il était possible de pirater à distance des stimulateurs cardiaques. Depuis, des hackers ont montré qu'ils étaient capables de prendre le contrôle de pompes à insuline au moyen de signaux radio et de déclencher l'injection d'insuline dans le système sanguin des patients.

Les infrastructures physiques sont aussi menacées. Le virus informatique Stuxnet l'a montré en 2010 en causant la destruction des centrifugeuses d'enrichissement de l'uranium au sein d'une installation clandestine à Natanz, en Iran. Fruit supposé d'une collaboration coûteuse entre les États-Unis et Israël, Stuxnet a révélé qu'un code numérique suffit à perturber et détruire des systèmes physiques analogiques. Depuis, d'autres attaques l'ont confirmé. En décembre 2014, l'Office fédéral allemand de la sécurité des technologies de l'information a rapporté que des pirates avaient perturbé certains systèmes d'une aciérie, empêchant le haut-fourneau de s'arrêter et infligeant d'importants dégâts au système. Trois mois plus tôt, des pirates chinois avaient attaqué les sites web de l'Agence américaine d'observation océanique et atmosphérique (NOAA) qui traitent des données satellitaires servant entre autres à l'aviation et à la réaction aux catastrophes.

**La cybersécurité ne concerne pas seulement la sécurisation des ordinateurs, des réseaux ou des serveurs web**

En d'autres termes, la cybersécurité ne concerne pas seulement la sécurisation des ordinateurs, des réseaux ou des serveurs web. Il ne s'agit pas juste de sécuriser des « secrets » (comme si nous en avions encore beaucoup pour Google et Facebook !). La bataille du cyberespace concerne la protection des objets, des infrastructures et des processus. Le danger encouru est la subversion et le sabotage des technologies que nous utilisons tous les jours : nos automobiles, distributeurs bancaires et appareils médicaux ; nos réseaux électriques, satellites de communication et réseaux téléphoniques. La cybersécurité vise à protéger notre mode de vie.

## Des vulnérabilités entretenues

Sécuriser le cyberespace confronte les gouvernements à des conflits profonds. De nombreuses agences fédérales, dont le Département de la sécurité intérieure des États-Unis, ont un réel intérêt à protéger les sociétés nationales et les citoyens des cyberattaques. Mais d'autres entités gouvernementales ont intérêt que le réseau mondial reste criblé de vulnérabilités. Des groupes clandestins tels que la NSA, l'Agence de sécurité américaine, investissent des millions pour trouver et maîtriser des failles techniques qui permettraient à un attaquant de prendre le contrôle d'un système.

La vulnérabilité de sécurité des uns est l'arme secrète des autres. Prenons le bug Heartbleed. Si vous avez utilisé Internet au cours des cinq dernières années, votre information a probablement été cryptée et décryptée par des ordinateurs équipés du logiciel OpenSSL. SSL est la technologie derrière les icônes en forme de cadenas qui signalent les sites web sécurisés. La vulnérabilité Heartbleed était le résultat d'une erreur élémentaire de développement logiciel dans Heartbeat, une des extensions d'OpenSSL, d'où le nom *(voir l'encadré page 55)*. Exploitée, la faille donnait aux indiscrets un accès facile aux clés de chiffrement, noms d'utilisateurs et mots de passe, rendant illusoire toute sécurité offerte par le chiffrement SSL. OpenSSL a été vulnérable pendant deux ans avant que deux équipes distinctes de chercheurs

### L'AUTEURE

**Keren ELAZARI, spécialiste israélienne de la sécurité, est consultante en cybersécurité et chercheuse associée du groupe de travail Science, sécurité et technologie de l'université de Tel Aviv.**

### SUR LE WEB

**La conférence TED de Keren Elazari,** *Who are the hackers ?*, 2014 : www.ted.com/playlists/10/who_are_the_hackers


© 360b / Shutterstock.com


© Jstone / Shutterstock.com

en sécurité (l'une dirigée par Neel Mehta, expert en sécurité chez Google, et l'autre de Codenomicon, dont le siège est en Finlande) ne découvrent le bug. Quelques jours plus tard, le magazine *Bloomberg Businessweek* citait des sources anonymes affirmant que la NSA utilisait cette faille depuis des années pour le cyberespionnage.

Nombre d'États puissants ont affecté leurs meilleurs techniciens et des millions d'euros à la découverte et à l'exploitation de vulnérabilités telles que Heartbleed. Les gouvernements achètent aussi des bugs sur le marché libre, contribuant à soutenir l'industrie des failles de sécurité. Un nombre croissant d'entreprises, telles que Vupen Security, à Montpellier, et Exodus Intelligence, à Austin, se spécialisent dans la découverte et la commercialisation de ces précieux bugs. Certains gouvernements dépensent même plus pour la recherche et le développement de capacités offensives que pour la défense contre les cyberattaques. Le Pentagone emploie nombre de chercheurs en vulnérabilités, et le budget de la NSA pour la cyberrecherche offensive est plus du double de celui consacré à la défense.

Cela ne signifie pas que les gouvernements ont des intentions malfaisantes ou qu'ils sont des ennemis de la cybersécurité. Les agences telles que la NSA recueillent des renseignements afin d'empêcher des actes abominables et il est logique qu'elles utilisent tout outil à leur disposition pour y parvenir. Toutefois, une étape importante de la sécurisation du cyberespace consistera à soupeser avec honnêteté les coûts et avantages de l'entretien des vulnérabilités par les agences gouvernementales. Une autre clé de la réussite sera de tirer le plein parti du pouvoir des gouvernements, qui peuvent par exemple obliger des entreprises et autres organismes à partager leurs informations sur les cyberattaques.

Les banques, en particulier, auraient tout intérêt à le faire, car les attaques sur les institutions financières suivent d'ordinaire un schéma prévisible : quand les criminels trouvent un angle d'attaque qui fonctionne avec une banque, ils l'essaient sur une autre, puis une autre… Toutefois, les banques évitent de divulguer des informations sur les attaques subies, car cela soulève des questions sur leur propre sécurité. Elles évitent aussi de communiquer avec leurs concurrentes ; dans certains cas même, les lois antitrust l'interdisent. Les gouvernements, en revanche, peuvent faciliter le partage d'informations entre banques. Ce partage est déjà mis en place aux États-Unis sous la forme du Centre de partage et d'analyse d'informations pour les services financiers (FS-ISAC), qui sert aussi les organismes financiers mondiaux. Et en février, Barack Obama a signé un décret présidentiel qui enjoint d'autres entreprises à partager leurs renseignements entre elles et avec le gouvernement.

**DEUX CYBERATTAQUES** qui ont marqué les esprits : le 24 novembre 2014, Sony Pictures Entertainment, filiale américaine du groupe japonais Sony, est piratée. De nombreuses données sont détruites, d'autres sont divulguées, notamment des films en postproduction. Quelques mois plus tôt, durant l'été 2014, des pirates ont volé les données personnelles de milliers de clients de la société américaine de portefeuille JP Morgan Chase.

## Les pirates à la rescousse

Tant que les hommes écriront des programmes, des vulnérabilités existeront. Sous la pression concurrentielle, les entreprises du secteur des technologies introduisent leurs produits sur le marché plus vite que jamais. Ces entreprises seraient bien avisées d'exploiter l'énorme ressource humaine que constitue la communauté mondiale des hackers. Au cours de l'année passée, catalysées par des événements tels que les révélations d'Edward Snowden sur la NSA, l'industrie technologique et la communauté des hackers ont commencé à accepter l'idée de travailler ensemble. À présent, des centaines d'entreprises voient l'intérêt d'embaucher des hackers en les attirant au moyen de programmes qui récompensent la découverte de bugs ou de vulnérabilités

**Aussi efficace soit-il, l'emploi de hackers n'est pas la seule façon d'éprouver la sécurité d'un système informatique. De plus en plus d'entreprises et d'institutions utilisent les méthodes formelles, et pour de bonnes raisons. La meilleure est sans doute que, le plus souvent, les hackers ne peuvent trouver des vulnérabilités que parmi un catalogue d'attaques connues, certes vaste, mais fini.**

Les méthodes formelles visent davantage. Issues de la recherche en informatique, elles consistent à modéliser tout ou partie d'un système informatique et à appliquer des algorithmes de vérification. Un tel algorithme prend en entrée le modèle conçu et une propriété de sécurité à vérifier, par exemple la confidentialité d'un message, et retourne une réponse oui (la propriété est vérifiée sur le modèle) ou non (une attaque est possible). La recherche d'une attaque est exhaustive : si une seule attaque existe contre la propriété dans le modèle, l'algorithme la trouvera.

Longtemps, les méthodes formelles ont semblé l'apanage de quelques chercheurs. Les industriels considéraient que les attaques trouvées étaient théoriques, c'est-à-dire inapplicables. C'est en train de changer, notamment pour la vérification des jetons de sécurité. Un jeton de sécurité est, typiquement, une clé USB qui fonctionne comme un coffre-fort pour vos clés secrètes. Vous la branchez dans votre ordinateur et, avec elle, vous pouvez vous authentifier et vous connecter à un site, chiffrer des documents confidentiels, déchiffrer ceux que l'on vous envoie. Vos clés secrètes ne sortent jamais du jeton : pour chiffrer un document, votre ordinateur l'envoie au jeton, qui le chiffre et le renvoie à l'ordinateur.

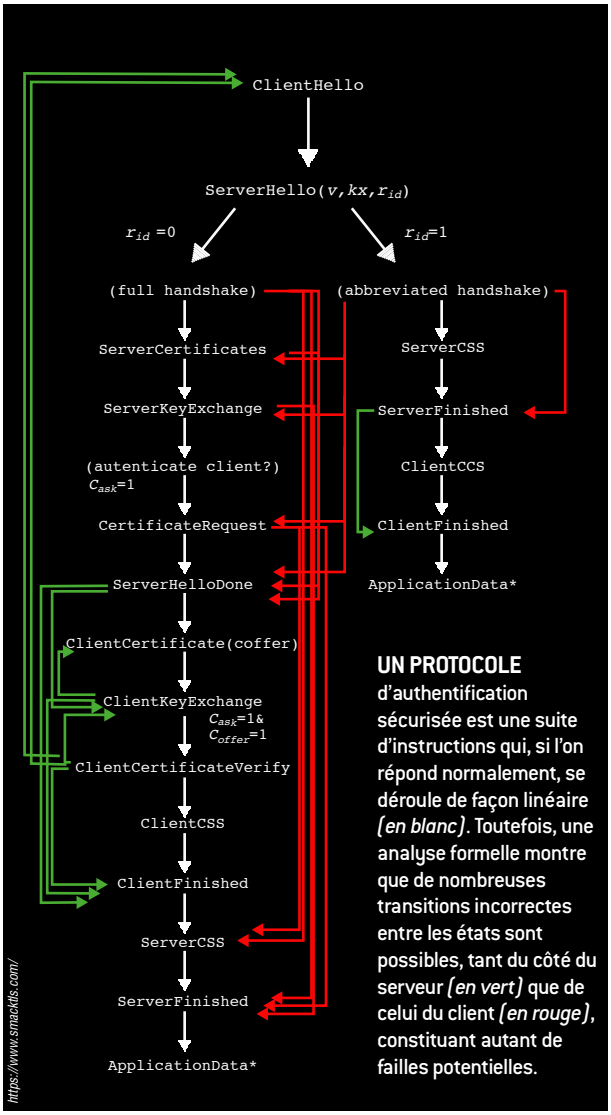
Pour déchiffrer votre message, votre correspondant a aussi besoin de la clé secrète utilisée. Il existe des moyens très malins pour fabriquer des clés secrètes communes à deux personnes et connues d'elles seules. Le protocole dit de Diffie-Hellman en est l'exemple type, mais il est coûteux en temps. En pratique, on obtient une fois pour toutes une clé K' par ce moyen et, pour toutes les autres clés K à partager, on demande au jeton d'encapsuler K en la chiffrant avec K'. Le jeton de votre correspondant déchiffre alors le message encapsulé à l'aide de K' et obtient K. Ainsi, votre clé K est certes sortie de votre jeton de sécurité, mais elle n'a circulé que sous forme chiffrée. De nouveau, la sécurité est assurée… Du moins, c'est ce que l'on pourrait croire.

En 2003, un jeune chercheur de Cambridge, Jolyon Clulow, a découvert une attaque théorique contre les jetons de sécurité. Elle fonctionne en deux étapes. On demande d'abord au jeton d'encapsuler la clé K avec la clé K'. On obtient, hors du jeton, une suite de bits M qui est le résultat du chiffrement de K avec K'. Jusque-là, rien d'utilisable. Mais si l'on demande au jeton de déchiffrer le message M avec la clé K', comme si M était un message chiffré que l'on venait de recevoir d'un correspondant, le jeton renvoie le message déchiffré : la clé K, lisible en clair…

De nombreuses précautions sont prises aujourd'hui pour éviter cette attaque, mais il y en a d'autres. Aussi, la jeune société française Cryptosense a développé un outil qui teste automatiquement votre jeton de sécurité *via* une méthode formelle, puis envoie un rapport de sécurité : pas de pirate à embaucher et une exhaustivité exceptionnelle dans la recherche d'attaques.

Autre exemple : la découverte en mars 2015 de l'attaque FREAK sur les protocoles sécurisés SSL/TLS. FREAK vous fait croire que vous disposez d'une connexion sécurisée avec des sites tels que Amazon ou PayPal, alors même que vous êtes connecté à un autre site, pirate. Même la NSA était vulnérable ! FREAK est une des attaques découvertes par des équipes communes à Inria et Microsoft, à l'aide de modèles fondés sur des machines à états *(des graphes tel celui ci-contre)*. Elles ont montré que les réalisations des protocoles faisaient bien davantage que ce qu'ils spécifiaient, et que ces possibilités supplémentaires étaient à l'avantage d'un attaquant.

Les méthodes formelles permettent d'assurer, sous certaines hypothèses, que votre système est sûr (s'il l'est). Notamment, la société française Prove&Run propose des solutions de sécurisation pour l'Internet des objets, les smartphones et tablettes, à destination des décideurs gouvernementaux ou des grandes entreprises qui ne peuvent se permettre d'être piratés. Ces solutions sont fondées sur des logiciels prouvés. Il faudrait un pirate bien malin pour les contourner.




**UN PROTOCOLE** d'authentification sécurisée est une suite d'instructions qui, si l'on répond normalement, se déroule de façon linéaire *(en blanc)*. Toutefois, une analyse formelle montre que de nombreuses transitions incorrectes entre les états sont possibles, tant du côté du serveur *(en vert)* que de celui du client *(en rouge)*, constituant autant de failles potentielles.

**– Jean Goubault-Larrecq**
*LSV, CNRS, ENS, Cachan*

– les *bug bounty programs* ou *vulnerability reward programs*. Ces programmes offrent des primes aux chercheurs indépendants qui signalent des vulnérabilités ou des problèmes de sécurité. Netscape Communications a créé le premier programme de prime à la découverte de bugs en 1995 afin de repérer les éventuels défauts du navigateur Netscape. Aujourd'hui, vingt ans plus tard, la recherche a montré que cette stratégie est une des mesures les plus rentables que la société et sa successeure, Mozilla, aient prises pour renforcer la sécurité. Les communautés privées et publiques de professionnels de la sécurité partagent leurs informations sur les logiciels malveillants, les menaces et les vulnérabilités. Elles créent ainsi une sorte de système immunitaire distribué.

À mesure que le cyberespace s'étend, constructeurs automobiles, entreprises de matériel médical, fournisseurs d'installations de cinéma à domicile et autres vont devoir raisonner comme des sociétés de cybersécurité. Cela suppose d'intégrer la sécurité dans la recherche et le développement, d'investir dans la sécurité des produits et des services dès la phase de conception, et non en fin de développement ou en réponse à des injonctions gouvernementales. Là encore, la communauté des hackers peut apporter sa contribution. En 2013, par exemple, les experts américains en sécurité Joshua Corman et Nicholas Percoco ont lancé le mouvement « I Am The Cavalry », pressant les pirates de s'engager dans une recherche responsable des failles de sécurité, notamment dans les domaines critiques tels que les infrastructures publiques, les équipements médicaux ou automobiles et les technologies domestiques connectées. Une autre initiative – BuildItSecure.ly –, à l'instigation des chercheurs en sécurité Mark Stanislav et Zach Lanier, vise à créer une plateforme pour développer des applications sécurisées de l'Internet des objets.

La bonne nouvelle est que ce système immunitaire distribué est de plus en plus solide. En janvier, Google a lancé un nouveau programme qui complète son programme de prime à la découverte de bugs, offrant des subventions pour encourager les chercheurs en sécurité à vérifier les produits de la compagnie. Cette décision montre que même des entreprises ayant recruté les meilleurs talents en technologie bénéficient du regard extérieur de pirates bien intentionnés. Certains gouvernements font de même. Ainsi, le Centre national néerlandais de cybersécurité a établi son propre programme de divulgation responsable, qui permet aux pirates de signaler des vulnérabilités sans risque de représailles juridiques.

Aux États-Unis, la mauvaise nouvelle est que certains éléments de l'approche cybersécuritaire du gouvernement pourraient *de facto* criminaliser les pratiques et les outils classiques de la recherche de vulnérabilités, ce qui affaiblirait le système immunitaire. Beaucoup d'acteurs de la sécurité craignent que la version actuelle de la loi *Computer Fraud and Abuse* (Fraude et malveillance informatiques) et les modifications proposées donnent une définition si large du piratage que le simple fait de cliquer sur un lien vers un site web contenant des fuites ou des informations volées soit considéré comme du trafic de biens volés. Cette criminalisation du travail des chercheurs indépendants nous ferait du tort à tous et aurait peu d'effet sur les criminels mus par le profit ou l'idéologie.

## Quelques règles de cyberhygiène

Les prochaines années pourraient être critiques. Le nombre de violations de données va augmenter et un ardent débat aura certainement lieu pour savoir quel pouvoir sur le monde numérique céder aux gouvernements en échange de sécurité. En fait, on ne pourra sécuriser le cyberespace sans combiner des solutions de diverses natures : techniques, légales, économiques et politiques. Et cela dépend aussi de nous, le grand public. En tant que consommateurs, nous devrions exiger que les entreprises rendent leurs produits plus sûrs. En tant que citoyens, nous devrions tenir nos gouvernements pour responsables quand ils affaiblissent volontairement la sécurité. Et en tant que points individuels de failles potentielles, nous avons la responsabilité de sécuriser nos installations.

Pour se défendre, il existe des mesures simples, telles que mettre à jour nos logiciels, utiliser des sites Web sécurisés et activer l'authentification à deux facteurs sur nos comptes de courriel et de réseaux sociaux. Mais cela suppose aussi d'être conscient que chacun de nos appareils est un nœud d'un vaste système et que les choix que nous faisons à notre petite échelle peuvent avoir des effets bien plus importants. La cybersécurité est comme la santé publique. Lavez-vous les mains, vaccinez-vous, et vous ne transmettrez pas les infections. ■

## Le bug Heartbleed

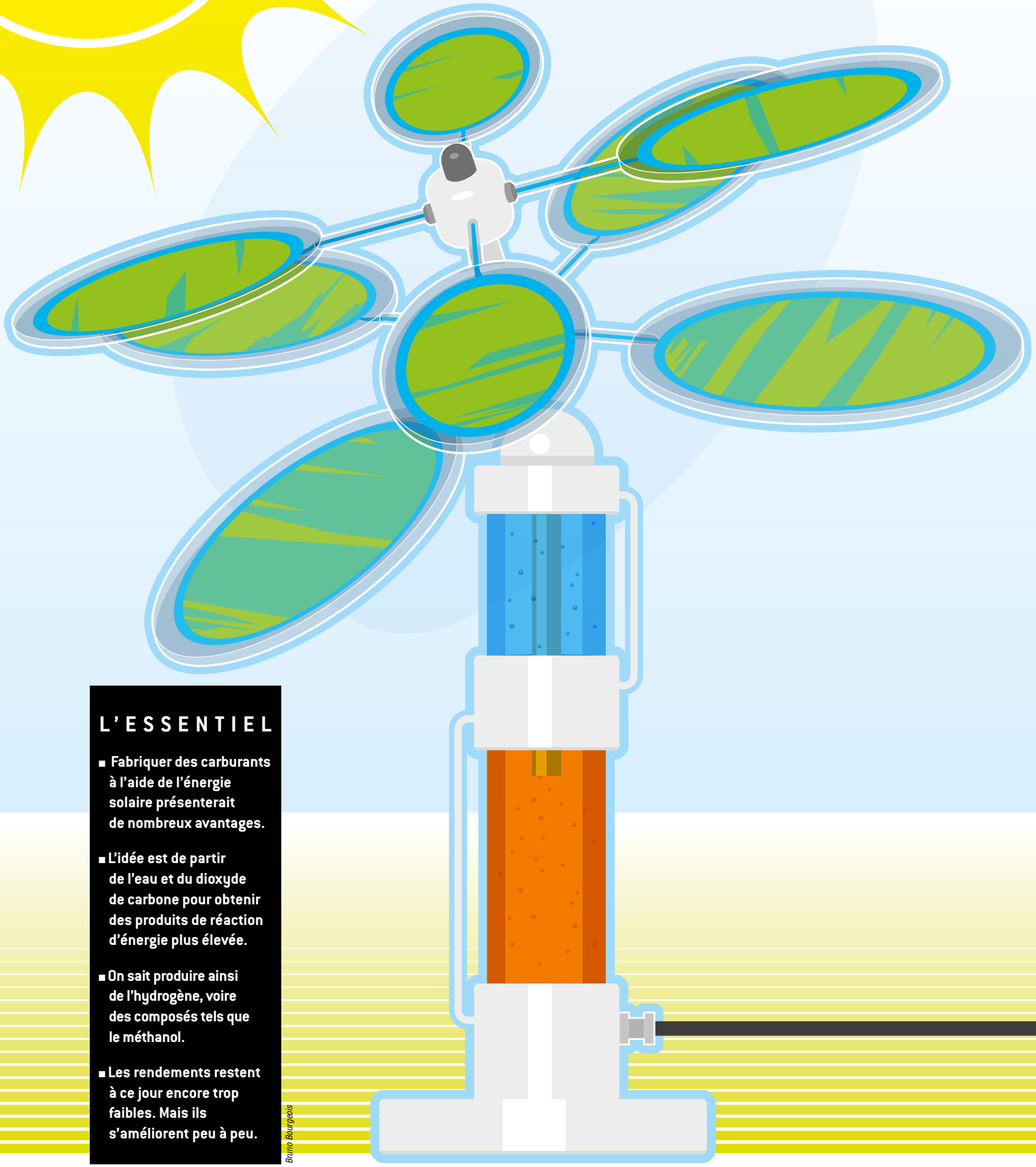
**Le 7 avril 2014, l'annonce de la faille Heartbleed dans la bibliothèque de cryptographie OpenSSL a soufflé un vent de panique chez les administrateurs systèmes. Durant deux ans, OpenSSL a présenté une vulnérabilité, introduite lors d'une amélioration. Il s'agit d'un bug d'implémentation. Heartbeat, une extension du protocole au cœur d'OpenSSL (SSL), récupère chez le client un message qui sert juste à vérifier que la connexion est active : il envoie un message basique au terminal client, qui lui répond. En utilisation normale, le message a deux parties : une suite d'octets et deux octets indiquant sa longueur. Mais dans Heartbleed, la longueur indiquée était bien plus grande que celle de la suite. En retour, le terminal client répondait un message de même longueur contenant la suite d'octets, comme en temps normal, mais aussi les octets suivants dans la mémoire, jusqu'à la longueur indiquée : avec de la chance, les identifiants utilisés…**

## ■ BIBLIOGRAPHIE


K. Zetter, **Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon**, Crown, 2014.

J. Healey (éd.), **A Fierce Domain : Conflict in Cyberspace, 1986 to 2012**, Cyber Conflict Studies Association, 2013.

**L'ère d'Internet**, *Dossier Pour la Science*, n° 66, janvier-mars 2010.



## L'ESSENTIEL

- Fabriquer des carburants à l'aide de l'énergie solaire présenterait de nombreux avantages.
- L'idée est de partir de l'eau et du dioxyde de carbone pour obtenir des produits de réaction d'énergie plus élevée.
- On sait produire ainsi de l'hydrogène, voire des composés tels que le méthanol.
- Les rendements restent à ce jour encore trop faibles. Mais ils s'améliorent peu à peu.

Bruno Bourgeois