

– 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 successeuse, 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 cyberspace 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

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.

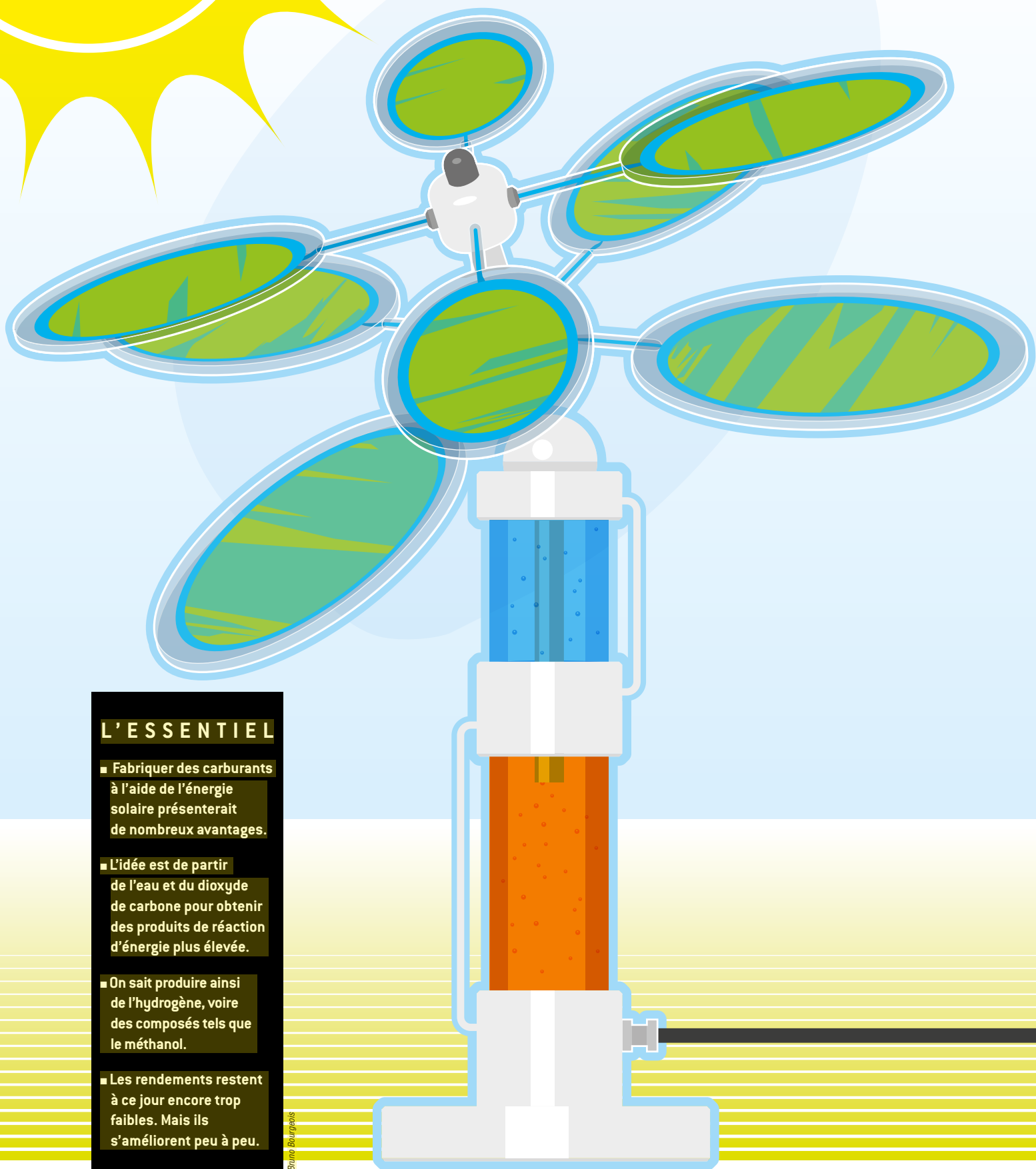
cybersécurité a établi son propre programme de divulgation responsable, qui permet aux pirates de signaler des vulnérabilités sans risque de représailles juridiques.

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 cyberspace 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 transmettez pas les infections. ■



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.

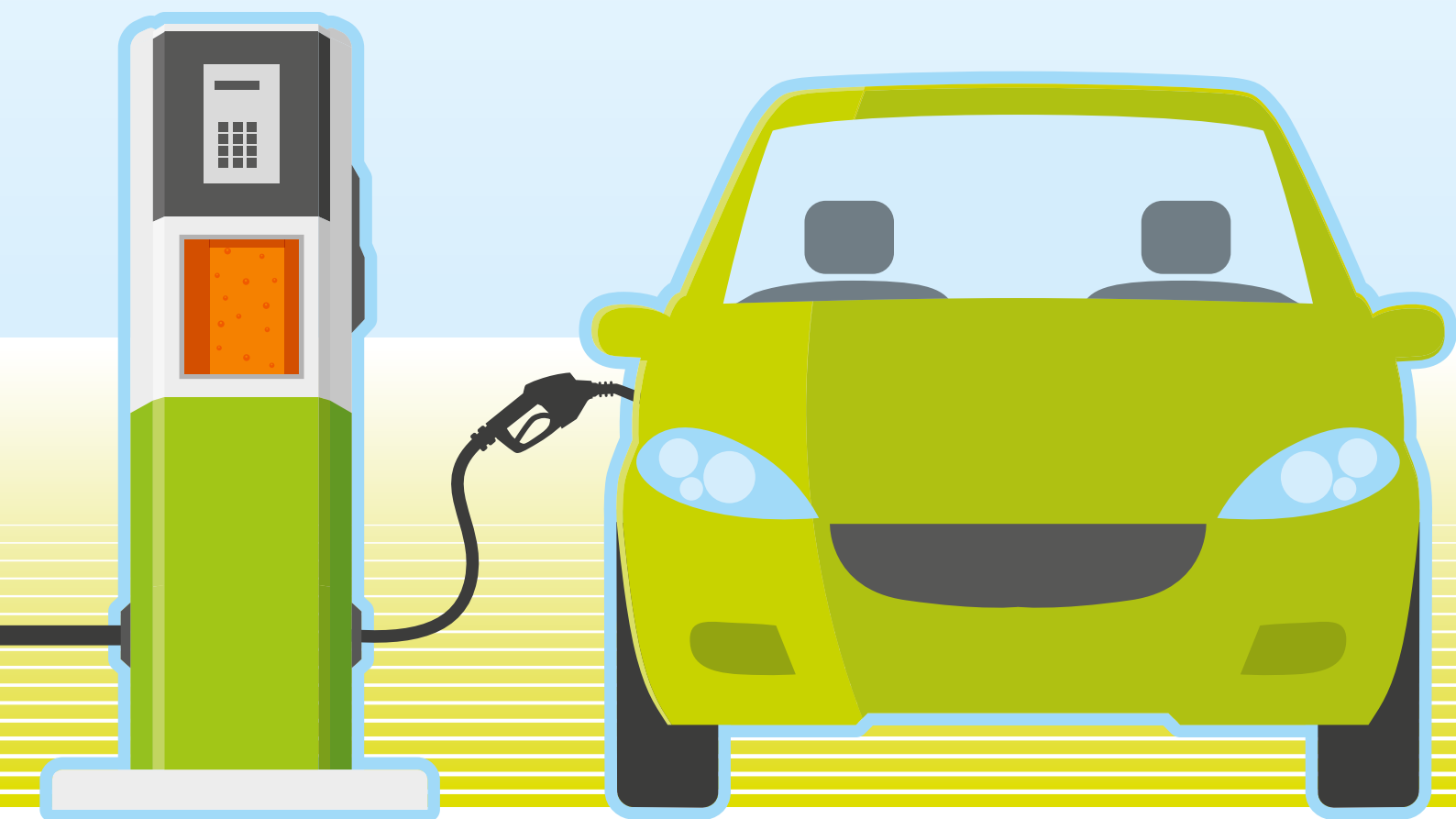
Bruno Bourgeois

DES CARBURANTS SOLAIRES

pour la transition énergétique

Antoine Fécant et Hervé Toulhoat

En recueillant le rayonnement du Soleil, il est possible de synthétiser des carburants à partir d'eau et de dioxyde de carbone. Les rendements de ces procédés de photosynthèse artificielle s'améliorent peu à peu.



LES AUTEURS



Antoine FÉCANT est ingénieur de recherche et chef de projet à la Direction catalyse et séparation d'IFPEN (IFP Énergies nouvelles), à Solaize.

Hervé TOULHOAT est directeur adjoint de la Direction scientifique d'IFPEN, à Rueil-Malmaison.

En ces temps où les questions de transition énergétique, de réchauffement climatique et de préservation de l'environnement sont parmi les grandes préoccupations internationales, l'utilisation de l'énergie solaire apparaît à l'évidence comme une voie à développer. L'exploitation directe par l'homme de cette énergie revêt aujourd'hui deux principales formes : d'une part, les procédés photovoltaïques, où le rayonnement solaire est capté et transformé en électricité ; d'autre part, les procédés photothermiques, où ce rayonnement est transformé en chaleur, à l'exemple des chauffe-eau solaires domestiques, très répandus dans certains pays.

Une troisième forme d'exploitation directe de l'énergie solaire est prometteuse et fait l'objet de recherches actives : la transformation de cette énergie en énergie chimique, les photons du Soleil servant à déclencher des réactions chimiques qui produisent des carburants. Les végétaux en appliquent le principe depuis leurs débuts sur Terre, au moyen de la photosynthèse. Aussi qualifie-t-on parfois de photosynthèse artificielle la synthèse de carburants par des procédés photochimiques mis au point par l'homme.

Quel est l'intérêt de fabriquer de tels « carburants solaires » ? Quelques chiffres seront utiles pour le comprendre. Le flux d'énergie qui nous parvient de notre étoile est gigantesque. L'énergie solaire absorbée

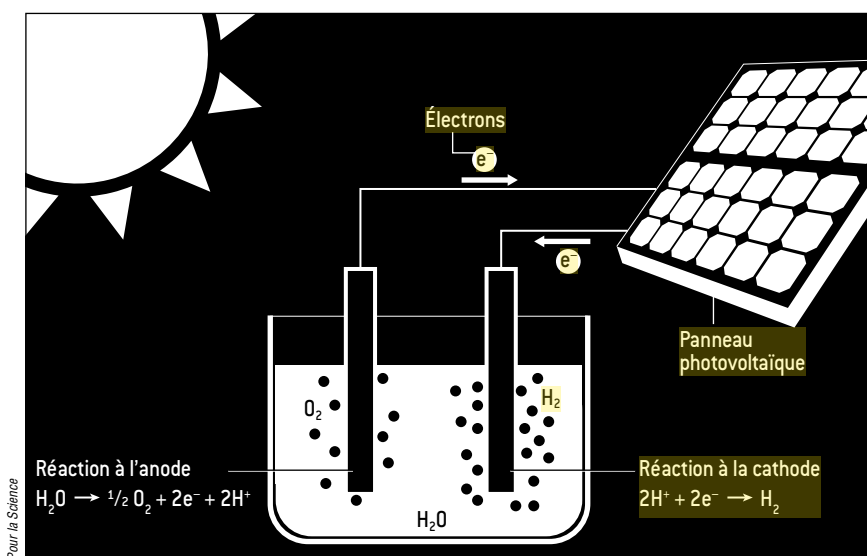
par la Terre est de l'ordre du milliard de térawattheures (1 TWh = 10^9 kilowattheures, ou kWh) par an. Ce chiffre est très supérieur à la consommation d'énergie de l'humanité, estimée à environ 150 000 TWh par an, dont près de 21 000 TWh sous forme d'électricité.

L'énergie solaire est certes abondante et renouvelable aux échelles de temps qui nous sont pertinentes, mais elle est dispersée : en moyenne, chaque mètre carré de la surface terrestre reçoit une puissance de 170 watts. Elle est en outre intermittente en raison des saisons, de l'alternance jour-nuit et des aléas météorologiques, et elle est inégalement répartie en latitude.

Une bonne forme de stockage de l'énergie

Pour pallier l'intermittence de l'énergie solaire, il faudrait stocker massivement l'énergie en laquelle on la transforme. Il s'agit là d'un défi qui se pose aussi pour l'énergie éolienne et qui mobilise beaucoup d'efforts de recherche et développement. Or les carburants constituent une forme de stockage chimique de l'énergie dont les avantages sont multiples. D'une part, ils sont facilement convertibles en énergie électrique, soit directement en alimentant des piles à combustible, soit indirectement en faisant tourner des turbines ou des moteurs à combustion interne. D'autre part, les carburants ont une très bonne densité de stockage (beaucoup d'énergie dans un petit volume et une faible masse), disposent d'un réseau de distribution bien développé et, pour ces deux raisons, conviennent aux utilisations mobiles – transports terrestre, aérien et maritime, informatique nomade, etc.

Comment fabriquer des carburants à partir du rayonnement solaire ? Nous nous limiterons ici aux stratégies non biologiques (quoique plus ou moins biomimétiques), à distinguer par exemple de la production de « biocarburants » à partir d'algues ou d'autres végétaux. Ces voies de photosynthèse artificielle mettent en œuvre l'eau (H_2O) et le dioxyde de carbone (CO_2), réactifs ayant de bas niveaux d'énergie, pour aboutir, en moissonnant l'énergie des photons solaires, à des produits de niveau d'énergie moyen plus élevé. Les produits de ces réactions photochimiques sont un carburant (ou plus précisément un combustible), à savoir de l'hydrogène (H_2) ou des composés organiques de formule $C_xH_yO_z$, et un comburant, le dioxygène (O_2).



UN PANNEAU PHOTOVOLTAÏQUE permet de produire de l'hydrogène (H_2) par électrolyse de l'eau : le panneau convertit le rayonnement solaire en électricité, laquelle assure, via deux électrodes plongées dans l'eau, la dissociation de l'eau en oxygène (O_2) et en hydrogène.