carbone organique durant cette période, sinon il n'aurait pu fournir l'énergie nécessaire à toutes ces innovations.

Dans un article récent, Seth Finnegan, de l'Université Stanford et de l'Institut de technologie de Californie, et ses collègues, dont je suis, avons tenté d'expliquer cette révolution marine du Mésozoïque sous un autre angle. Nous avons étudié, au cours du temps, les besoins énergétiques ou les demandes en nourriture probables d'un groupe prédominant dans les témoignages fossiles : les gastéropodes. Pour ce faire, nous avons combiné les informations issues des traces fossiles marines, des océans actuels – peu profonds comme profonds –, des données physiologiques provenant des espèces vivantes et, enfin, des équations mathématiques estimant la consommation d'énergie nécessaire à la vie d'un animal, c'est-à-dire l'énergie dont il a besoin pour son métabolisme.

Pour chiffrer les besoins de populations de gastéropodes dans un passé lointain, nous avons fait des extrapolations à partir de nos connaissances sur les gastéropodes actuels. En comparant les gastéropodes vivant avant et après la révolution marine du Mésozoïque, nous avons découvert que le besoin en énergie par individu s'était élevé d'environ 150 pour cent – un changement attribué en grande partie à l'augmentation de la taille des individus. Et si l'on ajoute à cette demande énergétique ne serait-ce que celle des carnivores marins, plus coûteux en énergie et dont la présence s'est accrue au Mésozoïque, on constate que le besoin en énergie après la révolution marine du Mésozoïque a dû être bien plus élevé.

Nous avons montré en outre que cette augmentation de la demande énergétique s'est produite des profondeurs océaniques jusqu'aux eaux côtières. Par conséquent, pour permettre cette augmentation, la productivité de l'océan a forcément dû s'accroître considérablement il y a 200 à 100 millions d'années.

Un avenir incertain

Aujourd'hui, la Terre entre dans une nouvelle période de turbulences. Alors que les émissions de gaz à effet de serre modifient le climat de notre planète, de plus en plus de preuves indiquent que nous avons déjà modifié la production et les flux du carbone dans les océans. Des travaux récents montrent des réductions de 50 pour cent de la production de phytoplancton dans certaines régions océaniques et des augmentations de 50 pour cent dans d'autres. Daniel Boyce, de l'Université Dalhousie, aux États-Unis, et ses collègues ont récemment rapporté que la production de phytoplancton a globalement décliné au cours du siècle dernier. Cette redistribution et la diminution de la quantité de carbone à la surface de l'océan pourraient modifier la nature des fonds marins de façon importante ces prochaines décennies, aux côtés de la surpêche, de la pollution, de l'exploitation minière, du réchauffement et de l'acidification.

Les organismes des profondeurs vivent dans des conditions environnementales extrêmes de température, de pression et, bien sûr, d'alimentation. À l'échelle des individus comme à celle des écosystèmes, des transformations écologiques et évolutives extraordinaires ont permis une adaptation à ces conditions extrêmes. Alors que l'activité humaine modifie toujours plus les fonds marins, les espèces qui les peuplent vont-elles s'adapter ou disparaître ? La question est ouverte. ■

La Niña, qui changent les températures de surface de l'océan Pacifique tropical, peuvent aussi modifier la répartition de la production planctonique en surface. Auraient-ils par là-même une influence sur la diversité de la faune ? Pour le savoir, un site appelé station M – situé à 4000 mètres de profondeur, au large de Santa Barbara, en Californie – a été surveillé pendant presque deux décennies. Des travaux effectués à la station M par Henry Ruhl et Ken Smith, de l'Institution Scripps d'océanographie et de l'Institut de recherche de l'Aquarium de Monterey Bay, aux États-Unis, montrent que lorsque des oscillations, dues à El Niño et à La Niña, apparaissent dans les températures de surface du Pacifique, la quantité de plancton varie de façon concordante. Et la diversité et l'abondance de la mégafaune et de la macrofaune des profondeurs changent également.

Ces deux séries d'études exceptionnelles confortent l'idée que les gradients de diversité des espèces en fonction de la latitude sont en partie dues à la variabilité de production du plancton en surface. Elles ont aussi mis au jour une répartition de la biodiversité dans les profondeurs en fonction du temps qui établit un lien encore plus fort entre la production en surface et la vie en eaux profondes.

L'AUTEUR

Craig McCLAIN est directeur scientifique adjoint du Centre national de synthèse sur l'évolution de Durham, en Caroline du Nord aux États-Unis, et rédacteur en chef du blog scientifique *Deep-Sea News*, deepseanews.com.

Article publié avec l'aimable autorisation de *American Scientist*.

✔ BIBLIOGRAPHIE

S. Finnegan *et al.*, **Escargot through time : an energetic comparison of marine gastropod assemblages before and after the Mesozoic Marine Revolution,** *Paleobiology*, vol. 37, pp. 252-269, 2011.

C. McClain et J. Barry, **Habitat heterogeneity, biogenic disturbance, and resource availability work in concert to regulate biodiversity in deep submarine canyons,** *Ecology*, vol. 91, pp. 964-976, 2010.

C. McClain *et al.*, **The island rule and the evolution of body size in the deep sea,** *Journal of Biogeography*, vol. 33, pp. 1578-1584, 2006.

H. A. Ruhl et K. L. Smith, **Shifts in deep-sea community structure linked to climate and food supply,** *Science*, vol. 305, pp. 513-515, 2004.

P. Geistdoerfer, **La vie dans les abysses**, Belin, 1995.

© Pour la Science - n° 407 - Septembre 2011

Plongés dans le noir par un virus ?

David Nicol

Des virus informatiques ont mis hors service certains systèmes de contrôle industriels. Le réseau électrique pourrait être la prochaine cible.

Vincent LaForet Redux Pictures

Durant l'été 2010, les médias ont révélé qu'un virus avait paralysé les installations d'enrichissement d'uranium iraniennes de Natanz, pourtant hautement sécurisées. La plupart des virus se répandent partout où ils le peuvent, mais celui-ci, nommé *Stuxnet*, avait une cible bien particulière, non connectée à Internet. *Stuxnet* a été placé sur une clef USB, remise à un technicien qui ne se doutait de rien et qui l'a branchée sur un ordinateur faisant partie d'une installation sécurisée. Une fois introduit, le virus s'est répandu silencieusement pendant des mois, à la recherche d'un ordinateur connecté à un composant électronique banal : un contrôleur logique programmable. C'est un petit boîtier en plastique rempli d'électronique, couramment utilisé pour contrôler les rouages des installations industrielles : valves, engrenages, moteurs et autres interrupteurs.

Les contrôleurs électroniques dans lesquels *Stuxnet* s'est introduit étaient associés aux centrifugeuses à uranium, élément clef des ambitions nucléaires iraniennes. Des milliers de ces centrifugeuses traitent le minerai d'uranium pour en extraire l'uranium enrichi nécessaire à la fabrication d'armes nucléaires. Dans les conditions de fonctionnement normal, ces centrifugeuses tournent tellement vite que leurs bords externes se déplacent juste au-dessous de la vitesse du son (environ 1 230 kilomètres par heure). *Stuxnet* a accéléré la rotation des centrifugeuses jusqu'à ce que leur bord atteigne pratiquement 1 600 kilomètres par heure, vitesse où le rotor a de fortes chances de voler en éclats. Et pendant ce temps, il envoyait de faux signaux aux systèmes de contrôle, indiquant que tout était normal. De fait, bien que l'étendue exacte des dégâts iraniens reste floue, le virus a au moins en partie atteint sa cible : l'Iran a dû remplacer début 2010 environ 1 000 centrifugeuses sur le site d'enrichissement de Natanz.

Le virus *Stuxnet* illustre à quel point les installations industrielles sont vulnérables face à la menace d'une cyberattaque. Le virus a visé et détruit des équipements sécurisés, et il a échappé à la détection pendant des mois. Cette attaque serait l'œuvre d'Israël, peut-être avec l'aide des États-Unis. Mais de nombreux États ou groupes terroristes pourraient utiliser une technologie similaire contre des infrastructures civiles critiques n'importe où dans le monde.

L'ESSENTIEL

- **Tous les composants du réseau de distribution de l'électricité sont aujourd'hui contrôlés par ordinateur. C'est la plus grande infrastructure physique interconnectée par de l'électronique.**
- **Le virus *Stuxnet*, qui a endommagé des installations nucléaires iraniennes, a montré à quel point les machines sont vulnérables face à un logiciel malveillant.**
- **Le réseau électrique, plus vaste, a encore plus de points faibles. Une attaque coordonnée pourrait mettre à terre une grande partie du réseau électrique d'un pays.**
- **Des mesures commencent à être prises pour renforcer la sécurité.**

© Pour la Science - n° 407 - Septembre 2011

Et malheureusement, les réseaux électriques sont bien plus faciles à infiltrer qu'une installation d'enrichissement d'uranium. Le réseau électrique américain, ou de tout autre pays développé, est constitué de milliers d'unités interconnectées qui fonctionnent en coordination étroite. En un sens, c'est la plus grosse machine jamais construite : un circuit électrique géant qui transporte l'énergie depuis les centrales jusqu'aux ampoules, aux réfrigérateurs et autres machines à des milliers de kilomètres à la ronde. C'est une machine ajustée avec une grande précision. Le courant qui circule dans le réseau pour satisfaire aux besoins d'un pays augmente et diminue en suivant exactement la demande. Les générateurs fournissent un courant alternatif en phase avec l'ensemble du réseau. Et si la panne d'un seul composant a des répercussions limitées sur ce vaste circuit, une cyberattaque coordonnée en de multiples points critiques du réseau électrique pourrait endommager les équipements au point de paralyser un pays pour des semaines, voire des mois.

Étant donné la taille et la complexité du réseau électrique, il faudrait beaucoup de temps et d'efforts pour mettre sur pied une attaque coordonnée. *Stuxnet* était le virus informatique le plus avancé jamais vu, sans doute le fruit de services secrets. Mais le code de *Stuxnet* est maintenant en libre accès sur Internet, ce qui augmente le risque qu'un groupe terroriste l'adapte pour attaquer une nouvelle cible ! Un groupe technologiquement peu avancé, comme Al Qaida, n'a probablement pas l'expertise nécessaire pour infliger des dommages significatifs au réseau électrique. Mais ce n'est pas le cas des *hackers* qui louent leurs services en Chine ou dans les pays de l'ex-Union soviétique.

Même des réseaux non reliés à Internet sont vulnérables

Il y a un an, j'ai participé à un exercice simulant une cyberattaque fictive sur le réseau électrique. Parmi les participants se trouvaient des représentants des entreprises de distribution de l'électricité, des agences gouvernementales et de l'armée. Dans ce test, des logiciels malveillants s'introduisaient dans un certain nombre de postes électriques (des installations qui servent à la fois à la transmission et à la distribution d'électricité), mettant hors d'usage les dispositifs qui assurent une tension constante. À la fin de l'exercice, une demi-douzaine de postes avaient été détruits, privant d'électricité pour plusieurs semaines tout un État de l'Ouest.

Des ordinateurs contrôlent le réseau à tous les niveaux, depuis les générateurs à combustible fossile ou les centrales nucléaires jusqu'aux lignes de transport urbain. La plupart de ces ordinateurs utilisent des systèmes d'exploitation grand public comme *Windows*, ce qui les rend presque aussi vulnérables que votre micro-ordinateur aux virus informatiques.

Un virus comme *Stuxnet* est efficace principalement pour trois raisons : les systèmes d'exploitation considèrent *a priori* que les logiciels qui s'exécutent sont légitimes ; ils présentent souvent des failles qui autorisent l'intrusion d'un virus ; et les installations industrielles permettent rarement d'utiliser des protections disponibles pour le grand public.

Même en sachant tout cela, un ingénieur système aurait jusque récemment écarté d'un revers de la main la possibilité qu'un logiciel malveillant lancé à distance puisse parvenir aux contrôles critiques

du réseau électrique, puisque ce système n'est pas directement connecté à Internet. Mais depuis, *Stuxnet* a démontré que les réseaux sans connexion permanente vers l'extérieur sont eux aussi vulnérables. Les virus peuvent par exemple se propager physiquement *via* des clefs USB utilisées par des employés. Même la plus petite porte dérobée peut servir d'entrée pour un cambrioleur entreprenant.

Prenons le cas d'un poste électrique. De tels postes reçoivent des courants à haute tension venant d'une ou plusieurs centrales, les synchronisent, abaissent la tension et les répartissent entre de multiples lignes pour la distribution locale. En cas de panne sur une de ces lignes, un disjoncteur coupe le courant. Toute l'électricité envoyée dans cette ligne est alors répartie entre les autres lignes. Si les lignes de distribution sont proches de leur limite de capacité, une attaque qui coupe la moitié des lignes et maintient les autres ouvertes a toutes les chances de surcharger ces dernières.

Des portes d'entrée multiples

Ces disjoncteurs sont encore aujourd'hui équipés de modems auxquels les techniciens peuvent se connecter. Or il n'est pas difficile de trouver ces numéros. Les pirates ont inventé depuis longtemps des programmes pour composer tous les numéros de téléphone d'un central téléphonique et repérer ceux auxquels un modem répond. Quand cela est combiné à une faible protection, comme des mots de passe bien connus ou pas de mot de passe du tout, un attaquant peut utiliser ces modems pour s'introduire dans le réseau d'un poste électrique. De là, il pourrait configurer les disjoncteurs de façon à ce qu'ils passent outre une situation dangereuse, au lieu d'ouvrir le circuit.

Les nouveaux systèmes ne sont pas plus sûrs. De plus en plus, les dispositifs déployés dans les postes électriques communiquent entre eux par ondes radio à faible puissance. Celles-ci ne s'arrêtent cependant pas aux murs du poste électrique. Un pirate peut s'introduire dans le réseau en se cachant dans les parages avec son ordinateur. Les réseaux Wi-Fi cryptés sont plus sûrs, mais un attaquant compétent peut quand même casser le cryptage avec des logiciels faciles à se procurer. De là, il pourrait lancer une « attaque de l'homme du milieu » qui fait transiter par son ordinateur toutes les communications entre deux ordinateurs légitimes, ou faire accepter son ordinateur comme légitime. Il serait alors en mesure d'envoyer des messages de contrôle frauduleux qui perturberaient le fonctionnement des disjoncteurs.

Une fois qu'un virus s'est introduit dans un réseau, sa première consigne est en général de se répandre le plus possible. Là encore, *Stuxnet* illustre des stratégies bien connues. Il a tiré profit d'un mécanisme du système d'exploitation *Windows*, qui lit et exécute un fichier nommé autoexec.bat à chaque fois qu'un utilisateur s'identifie pour localiser des pilotes de périphériques, lancer un antivirus, ou d'autres fonctions de base. Mais le système suppose que tout fichier ayant le bon nom est un code fiable. Il suffit ainsi de modifier le fichier autoexec.bat pour qu'il exécute le code malveillant.

Les attaquants peuvent aussi exploiter la structure du marché de l'électricité. Dans le cadre de la dérégulation, l'électricité est produite, transportée et distribuée par des compagnies concurrentes, dans le cadre de contrats qui portent sur diverses échéances, obtenus dans des enchères en ligne. La branche commerciale d'une compagnie doit recevoir en permanence des informations en temps réel de sa branche d'exploitation afin de faire des transactions intéressantes ; inversement, la branche exploitation doit savoir combien d'électricité elle doit produire pour répondre aux commandes de la branche commerciale. C'est là que se trouve le talon d'Achille. Un pirate pourrait pénétrer dans le réseau commercial, y dénicher des noms d'utilisateurs et des mots de passe, et utiliser ces identifiants pour accéder au réseau d'exploitation.

D'autres attaques pourraient se répandre en exploitant des scripts cachés dans des fichiers. On trouve des scripts partout (les fichiers PDF, par exemple, contiennent souvent des scripts qui gèrent l'affichage), mais ils représentent aussi un danger potentiel. Une entreprise de sécurité informatique estimait récemment que plus de 60 pour cent des attaques ciblées utilisent des scripts enfouis dans des fichiers PDF. Le simple fait de lire un fichier corrompu peut laisser entrer un attaquant dans votre ordinateur.

Imaginons qu'un attaquant pénètre dans un premier temps sur le site Web d'un fournisseur de logiciels et remplace un manuel en ligne par un faux manuel corrompu semblable au premier. Le cyberattaquant envoie alors à un ingénieur de la centrale électrique un message, qui va

ATTAQUES INFORMATIQUES, DÉGÂTS PHYSIQUES

À mesure que l'on relie les machines industrielles au réseau Internet, le potentiel de nuisance des pirates augmente. Les attaques recensées ces dix dernières années montrent que le réseau électrique n'est pas le seul point faible : tout ce qui comporte un circuit intégré peut être pris pour cible.

La centrale nucléaire de Davis-Besse (Ohio, États-Unis).

Avril 2000
Un ancien employé mécontent d'une entreprise de traitement de l'eau vole des composants radio et les utilise pour envoyer de fausses instructions aux équipements des égouts du Queensland, en Australie. Plus de 750 000 litres d'eaux usées sont déversées dans les parcs et les rivières du secteur.

2000 2001

© Pour la Science - n° 407 - Septembre 2011

inciter l'ingénieur à télécharger le manuel piégé. Ce faisant, l'ingénieur ouvre involontairement les portes de sa centrale au cheval de Troie. Une fois que le fichier corrompu se trouve à l'intérieur, l'attaque proprement dite peut commencer.

Désynchroniser, surcharger, ralentir

Un programme malveillant qui a réussi à s'introduire dans un réseau de contrôle peut émettre des instructions aux conséquences dévastatrices. En 2007, le Département de la Sécurité intérieure des États-Unis a simulé une cyberattaque au Laboratoire national de l'Idaho. Au cours de cet exercice, nommé *Aurora*, un ingénieur jouant le rôle de pirate s'est frayé un chemin jusque dans un réseau connecté à un générateur de taille moyenne. Comme tous les générateurs, il produit du courant alternatif. L'attaquant a émis une rapide séquence d'instructions marche/arrêt aux disjoncteurs d'un générateur test du Laboratoire, qui ont eu pour effet de le désynchroniser par rapport au courant alternatif du réseau. À « contre-courant » du réseau, le générateur n'a pas résisté longtemps : une vidéo aujourd'hui déclassifiée montre l'énorme machine d'acier tremblant comme si un train l'avait heurtée. Quelques secondes plus tard, la pièce était envahie de fumée.

Les systèmes industriels peuvent aussi tomber en panne quand ils sont poussés au-delà de leurs limites. Des centrifugeuses qui tournent trop vite se désintègrent. Un attaquant pourrait faire en sorte qu'un générateur électrique produise une tension supérieure à ce que les lignes de transport peuvent supporter. La puissance excédentaire serait alors évacuée sous forme de chaleur, entraînant l'affaissement de la ligne, voire sa fusion. Si des lignes affaissées entrent en contact avec quoi que ce soit, cela peut créer un énorme court-circuit. Des relais de protection sont prévus pour empêcher de tels courts-circuits, mais une cyberattaque pourrait également modifier le fonctionnement de ces relais, de façon à infliger des dégâts. En outre, l'attaque pourrait aussi modifier l'information envoyée à la station de contrôle, empêchant les opérateurs de remarquer qu'il y a un problème, comme dans ces films où les cambrioleurs envoient au gardien des images de vidéosurveillance truquées.

Les stations de contrôle elles aussi sont vulnérables aux attaques. Les personnels en salle d'opérations suivent sur écran les données transmises par les postes électriques, puis émettent des instructions pour en modifier les paramètres de contrôle. Une station est souvent responsable du suivi de centaines de postes.

La communication entre les stations de contrôle et les postes électriques utilise des protocoles spécialisés qui peuvent eux-mêmes être vulnérables. Si un intrus parvient à lancer une attaque de l'homme du milieu, il peut insérer un message dans un échange ou corrompre un message existant, voire simplement injecter un message correctement formaté, mais hors contexte, pour induire une défaillance d'un ordinateur à l'une ou l'autre extrémité.

Une autre stratégie est de retarder les messages transitant entre les stations de contrôle et les postes électriques. D'ordinaire, le délai entre la mesure du courant dans un poste et la réaction par la station de contrôle est court (sinon, cela revient à conduire une voiture en regardant là où vous étiez il y a dix secondes !). Le manque de données sur la situation en temps réel du réseau était en partie responsable de l'immense panne de courant qui a frappé l'Amérique du Nord en 2003.

Pour la plupart de ces attaques, nul besoin de logiciel sophistiqué comme *Stuxnet* : la boîte à outils du pirate de base suffit. Par exemple, des pirates prennent fréquemment le contrôle de milliers d'ordinateurs de bureau auxquels ils font faire ce qu'ils veulent, formant un réseau de

Janvier 2003
Le virus informatique *Slammer* contourne de nombreux pare-feu pour infecter le centre de contrôle de la centrale nucléaire de Davis-Besse dans l'Ohio (États-Unis). Le virus se répand à partir de l'ordinateur d'un sous-traitant jusque dans le réseau commercial, d'où il gagne les ordinateurs contrôlant l'exploitation de la centrale, entraînant la panne de multiples systèmes de sécurité. La centrale était à l'époque hors réseau.

Mars 2007
Des agents du gouvernement américain simulent une cyberattaque, nommée *Aurora*, sur un générateur électrique au Laboratoire national de l'Idaho. Le générateur est détruit.

Janvier 2008
Un responsable de la CIA révèle que des pirates informatiques auraient souvent infiltré les services d'électricité hors des États-Unis, avec des tentatives d'extorsion. Dans au moins un cas, les pirates auraient réussi à couper l'alimentation électrique de plusieurs villes, non nommées.

Avril 2009
Selon le *Wall Street Journal*, des cyberespions de Chine, Russie et d'autres pays auraient pénétré le réseau électrique américain et y auraient laissé des logiciels pouvant être utilisés pour le mettre hors service.

Octobre 2010
Des responsables de la sécurité en Iran, en Indonésie et ailleurs signalent la découverte de *Stuxnet*, un virus conçu pour attaquer des systèmes de contrôle industriels fabriqués par *Siemens*, qui commandent les centrifugeuses iraniennes.

2002 2003 2004 2005 2006 2007 2008 2009 2010 2011

Mark Duncan AP Photo, Mark Peterson Redux Pictures, Ebrahim Norouzi AP Photo

« machines zombies », ou botnet. Le type le plus simple d'attaque par botnet consiste à inonder un site Internet de messages quelconques pour ralentir ou bloquer la circulation de l'information. Ces attaques par « déni de service » pourraient être utilisées pour ralentir le trafic entre les postes électriques et les stations de contrôle.

Des botnets pourraient également s'implanter au sein même des ordinateurs du réseau de postes électriques. En 2009, le botnet *Conficker* avait investi dix millions d'ordinateurs. Un tel botnet pourrait intégrer des ordinateurs des postes électriques, et son contrôleur pourrait alors leur faire exécuter simultanément telle ou telle instruction. D'après le Département de l'Énergie des États-Unis, la mise hors service de 200 postes de transmission soigneusement choisis, soit deux pour cent du total, mettrait à genoux 60 pour cent du réseau électrique.

Quand une entreprise comme *Microsoft* a connaissance d'une faille de sécurité de ses logiciels, elle fournit un correctif. Les utilisateurs du monde entier téléchargent ce correctif, mettent à jour leur logiciel et se protègent ainsi de la menace. Malheureusement, les choses ne sont pas aussi simples sur le réseau électrique.

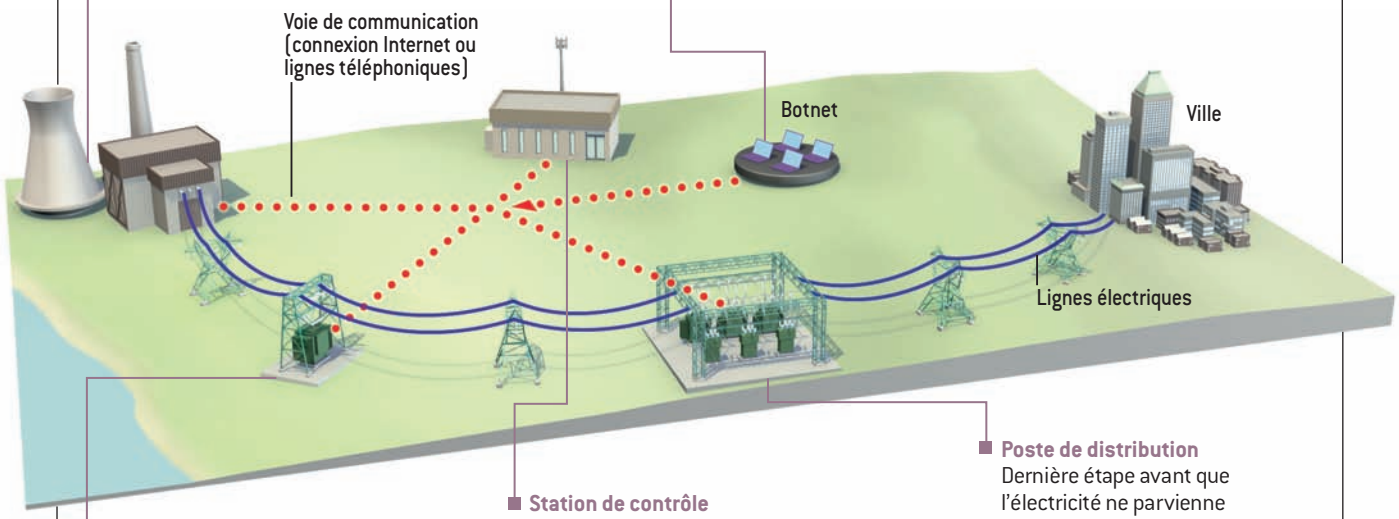
Même si le réseau électrique utilise du matériel et des logiciels grand public, les responsables informatiques des centrales électriques ne peuvent pas simplement corriger les logiciels défectueux quand des failles se révèlent. Les systèmes de contrôle

DES FAILLES DANS LE RÉSEAU

Le réseau électrique repose sur un équilibre complexe entre la quantité d'énergie dont les usagers ont besoin et la quantité produite par les centrales. Des dizaines de composants orchestrent la circulation de l'électricité sur des distances de centaines de kilomètres. Chacun de ces composants peut être mis à mal par des cyberattaquants. Voici quelques-uns des points les plus sensibles et comment ils pourraient être attaqués.

Centrale électrique
Que la centrale utilise du charbon, de l'uranium ou même l'énergie solaire, l'électricité injectée dans le réseau doit être un courant alternatif synchronisé avec le reste du réseau. Un attaquant pourrait envoyer des instructions à un générateur pour lui faire fournir un courant déphasé. Cela équivaut à passer la marche arrière alors que vous roulez sur une route à 80 kilomètres par heure : le générateur, opposé à l'inertie du réseau, va griller.

Transmission de l'information
La station de contrôle doit savoir à la seconde près ce qui se passe à chaque étape du transport pour que les techniciens puissent réagir et adapter les différents paramètres du réseau. Des pirates contrôlant des milliers d'ordinateurs (un botnet) pourraient ralentir les communications en inondant la station de contrôle de messages inutiles (attaque par déni de service). Les opérateurs prendraient des décisions en s'appuyant sur des informations anciennes, ce qui peut être inadapté à la situation réelle.



Poste de transmission
Le courant livré par les centrales électriques est à très haute tension, afin de limiter les pertes d'énergie durant le transport, dues à la résistance électrique. Les postes de transmission sont la première étape pour abaisser cette tension. De nombreux postes parmi les plus anciens sont équipés de modems auxquels les techniciens se connectent pour effectuer la maintenance. Des pirates peuvent les utiliser pour accéder aux réglages sensibles et les modifier.

Station de contrôle
Centres névralgiques du réseau électrique, les stations de contrôle surveillent l'ensemble des conditions de fonctionnement. C'est également là qu'est gérée l'adéquation entre l'offre et la demande. Quand la demande augmente, une entreprise mobilise plus de capacité de production pour répondre aux besoins. Bien que la salle d'opérations d'une station de contrôle ne soit pas censée être raccordée à Internet, la branche commerciale de la compagnie l'est. Un pirate peut s'infiltrer dans le réseau commercial et passer dans le réseau d'exploitation pour attaquer des systèmes de contrôle critiques.

Poste de distribution
Dernière étape avant que l'électricité ne parvienne aux particuliers et aux entreprises, ces postes peuvent combiner le courant provenant de plusieurs centrales différentes et l'envoyer sur des centaines de lignes plus petites. Les stations les plus récentes sont parfois équipées de dispositifs de communication radio ou Wi-Fi. Un intrus qui se cache à proximité du poste pourrait intercepter les échanges et leur substituer des instructions illégitimes.

George Retseck

© Pour la Science - n° 407 - Septembre 2011

du réseau ne peuvent pas être arrêtés pour maintenance ne serait-ce que quelques heures par semaine : ils doivent fonctionner en permanence. Les opérateurs sont aussi assez conservateurs. Les réseaux de contrôle sont en place depuis longtemps, et les opérateurs ont leurs routines qui ont fait leurs preuves. Ils se méfient de tout ce qui risquerait de menacer la disponibilité ou d'interférer avec l'exploitation normale.

Sécuriser le réseau d'ici 2020

Le NERC *(North American Electric Reliability Corporation)*, un organisme de tutelle des opérateurs du réseau américain, a édicté un ensemble de normes destinées à protéger l'infrastructure face à un danger clair et immédiat. Les entreprises de service public doivent maintenant identifier leurs dispositifs critiques et faire la preuve auprès d'auditeurs nommés par le NERC qu'ils sont capables de les protéger des intrusions.

Mais les audits de sécurité, comme les audits financiers, ne sont jamais exhaustifs. Les détails techniques audités ne sont qu'une sélection de points, et la conformité se limite à ce que l'auditeur voit.

La stratégie de protection la plus courante consiste à dresser une sorte de ligne Maginot électronique. La première ligne de défense est un « pare-feu », un dispositif à travers lequel passent tous les messages électroniques. Chaque message possède un en-tête indiquant d'où il vient, où il va, et le protocole utilisé pour l'interpréter. Sur la base de ces informations, le pare-feu laisse passer certains messages et en bloque d'autres. Les agences de certification doivent s'assurer que les centaines ou les milliers de pare-feu d'un site sensible sont correctement configurés. Pour ce faire, ils identifient quelques éléments critiques, se procurent les fichiers de configuration du pare-feu et essayent de déterminer manuellement comment un pirate traverserait le pare-feu.

Mais les pare-feu sont tellement complexes qu'il est difficile d'examiner la multitude de possibilités. Des outils automatisés seraient utiles. Notre équipe de l'Université de l'Illinois à Urbana-Champaign a développé le *Network Access Policy Tool*, aujourd'hui utilisé par des entreprises de service public et des équipes d'évaluation. Ce logiciel libre n'a besoin que des fichiers de configuration des pare-feu d'une entreprise. Il a d'ores et déjà permis d'identifier un certain nombre de chemins d'accès inconnus ou tombés dans l'oubli, que des attaquants auraient pu exploiter.

Le Département américain de l'Énergie a établi une feuille de route pour renforcer la sécurité du réseau d'ici à 2020. L'un des buts est de mettre au point un système qui reconnaît une tentative d'intrusion et qui y réagit automatiquement. Cela bloquerait un virus de type *Stuxnet* dès sa sortie de la clef USB. Mais comment un système d'exploitation peut-il savoir à quels programmes faire confiance ?

Une solution serait d'utiliser une technique cryptographique appelée fonction de hachage à sens unique. Une fonction de hachage prend un nombre immensément grand, par exemple le nombre de 0 et de 1 d'un fichier informatique, et le convertit en un nombre beaucoup plus petit, qui joue le rôle de signature. Il est très improbable que deux programmes différents et assez longs aient la même signature. Imaginez que chaque programme qui veut s'exécuter sur un système doive d'abord passer par la fonction de hachage. Sa signature est alors vérifiée par comparaison avec une liste de référence. Si elle ne correspond pas, l'attaque s'arrête là.

Le Département de l'Énergie recommande également d'autres mesures de sécurité, comme des vérifications de sécurité physiques aux postes de travail des opérateurs (des puces radio dans les badges d'identification, par exemple). Il souligne également le besoin d'exercer un contrôle plus strict sur les communications entre les dispositifs à l'intérieur du réseau électrique. La démonstration *Aurora* impliquait un programme malveillant qui faisait croire au dispositif de contrôle du générateur qu'il envoyait des instructions fiables...

Ces mesures nécessiteront du temps, de l'argent et des efforts, mais elles en valent la peine. Si nous voulons sécuriser le réseau électrique d'ici 2020, il va falloir accélérer le rythme. En espérant que d'ici là, il n'arrive rien de fâcheux. ■

LA MISE HORS SERVICE DE 200 POSTES DE TRANSMISSION

bien choisis, soit deux pour cent du total, mettrait à genoux 60 pour cent du réseau électrique américain.

L'AUTEUR

David NICOL est professeur au Département de génie électrique et informatique de l'Université de l'Illinois à Urbana-Champaign, aux États-Unis. Il est aussi directeur de l'*Information Trust Institute* de cette université.

✔ BIBLIOGRAPHIE

J.-Y. Marion et M. Kaczmarek, **Boulevard du cybercrime**, *Dossier Pour la Science* n °66, janvier-mars 2010, www.pourlascience.fr/u.php?s=cybercrime

J. Eisenhauer et *al*., **Roadmap to secure control systems in the energy sector**, *Energetics Incorporated*, janvier 2006. www.oe.energy.gov/csroadmap.htm

D. Geer, **Security of critical control systems sparks concern**, *IEEE Computer*, vol. 39, n°1, pp. 20-23, janvier 2006.

Trustworthy Cyber Infrastructure for the Power Grid, projet interuniversitaire financé par le Département américain de l'Énergie : www.tcipg.org

What Is the Electric Grid, and What Are Some Challenges It Faces?, Département américain de l'Énergie, www.eia.doe.gov/energy_in_brief/power_grid.cfm

✔ SUR LE WEB

Le portail gouvernemental français sur la sécurité informatique : http://www.ssi.gouv.fr/

La vidéo de l'exercice *Aurora* : http://bit.ly/pls407-video-aurora

HISTOIRE DES SCIENCES

L'affaire de la gale : histoire d'un concept scientifique

Au XIXe siècle, les médecins accusent un jeune docteur en médecine d'avoir falsifié ses travaux pour prouver l'existence du parasite de la gale. Leur argumentation révèle tous les obstacles qui les empêchaient d'envisager cette idée.

Danièle GHESQUIER-POURCIN

Comment les concepts scientifiques se construisent-ils ? Selon l'idée la plus répandue, leur marche est linéaire et sa vitesse est fonction du nombre d'individus qui se penchent sur le problème et du temps qu'ils lui consacrent. On croit aussi généralement qu'une découverte est le fait d'un seul individu : Flemming a découvert la pénicilline, Einstein la relativité, Darwin le phénomène d'évolution et Pasteur le vaccin contre la rage. Ces croyances sont fausses. Il suffit d'examiner l'histoire d'une découverte prise au hasard pour s'en persuader. La marche des idées n'est pas linéaire. Les concepts se construisent au gré de nombreux retours en arrière et d'apports par des voies indirectes, insoupçonnées auparavant, car la diversité est le seul artisan de la progression du savoir.

De plus, l'ordre des composants de la chaîne des idées qui forment le concept est important : par exemple, on ne pouvait expliquer le phénomène d'évolution sans reconnaître auparavant l'influence du milieu. Enfin, si l'on associe une découverte à une seule personne, c'est parce que l'on porte une attention particulière à celui qui sait rassembler les idées pour reconstituer le concept. D'où viennent ces idées ? Souvent de loin, apportées par d'autres individus qui ont une part dans la construction du concept, bien que celle-ci reste ignorée. En d'autres termes, le savoir est une construction collective qui ne se concrétise que lorsque le nombre d'éléments nécessaires est en présence dans un ordre déterminé. C'est ce que nous enseigne l'étude archéologique des nombreuses strates qui constituent le concept, comme nous allons le voir ici sur un exemple représentatif de cette marche de la science : l'histoire de la maladie, plus précisément d'une « maladie spécifique », la gale humaine.

Le sarcopte de Galès : une imposture ?

Parmi les différents types de maladies connus aujourd'hui – maladies spécifiques, de carence, génétiques, etc. –, la maladie spécifique, pathologie due à un agent externe « vivant » tel qu'un parasite, une bactérie ou un virus, fut la première à être élucidée. Ce type de maladie offrait plusieurs énigmes à résoudre : l'essence de la maladie, le rôle de l'animal, les conditions de sa pénétration dans l'organisme-hôte, son mode d'action dans le déclenchement de la maladie, son mode de vie à l'intérieur du corps malade, les mécanismes de la contagion et ceux mis en jeu physiologiquement pour se débarrasser de l'intrus, les thérapeutiques susceptibles d'aider le malade à recouvrer la santé.

Une de ces interrogations était primordiale : quelle était la cause de la maladie ? La réponse à cette question conditionnait celles à toutes les autres questions, en particulier celles relatives à la thérapeutique qui, dans la maladie spécifique, se confond avec la destruction de la cause. La cause était aussi la seule façon de définir la maladie au moyen d'une propriété qui lui était spécifique.

L'histoire de la gale humaine analysée ici inclut une affaire de fraude scientifique supposée qui n'a jamais été élucidée. Au travers de cette « affaire de la gale », que nous tenterons de clarifier, se dessinera l'itinéraire des idées qui constituent le concept de gale et celui de maladie spécifique en général.

L'affaire de la gale est d'habitude présentée comme une fraude scientifique qui aurait été commise, en 1812, par un étudiant nommé Jean-Chrysanthe Galès (1783-1854) pour sa thèse de médecine, sous la direction du médecin-chef de l'hôpital Saint-Louis de Paris, Jean-Louis Alibert, spécialiste des maladies de peau. Elle a été racontée de nombreuses fois, sans qu'aucune voix se soit jamais élevée pour défendre Galès, dont la culpabilité n'a pourtant jamais été démontrée.

La gale est caractérisée par de violentes démangeaisons, des boutons et des croûtes sur la peau. Aujourd'hui, on sait que la démangeaison est due à un arthropode de l'ordre des acariens, le sarcopte. Ce parasite creuse des sillons dans le derme afin d'y déposer ses œufs, sectionnant à la fois le derme et les petits vaisseaux qu'il trouve sur son chemin *(voir la figure 1)*. Le tissu réagit en formant de petites vésicules remplies d'un liquide séreux transparent, fait de fragments cellulaires et d'un peu de sang. Si la gale n'est pas soignée, ces vésicules grossissent et se remplissent de pus, devenant des pustules. Au début du XIXe siècle, les patients traités pour la gale dans les hôpitaux parisiens se trou-

© Pour la Science - n° 407 - Septembre 2011