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 4 000 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.

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.

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.**

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