

extrasolaires, à partir des années 1990, et des années avant que l'astronome Frank Drake ne présente son argument probabiliste concernant la rareté des civilisations capables de communiquer dans le cosmos, en 1961. L'extrapolation de données de l'observatoire spatial *Kepler* suggère que la Voie lactée contient probablement plus d'un milliard de planètes de la taille de la Terre dans les zones habitables d'étoiles de la taille du Soleil, ou plus petites.

Conscient des distances

Enfin, après quelques considérations sur les immenses distances en jeu, Churchill conclut que nous ne saurons peut-être jamais si ces planètes « hébergent des créatures vivantes, ou même des plantes ».

Churchill voit une opportunité immense pour l'exploration du Système solaire. « Un jour, peut-être même dans un avenir pas si lointain, il pourrait être envisageable de voyager jusqu'à la Lune, voire Vénus ou Mars », écrit-il. En revanche, note-t-il, le voyage et la communication interstellaires sont intrinsèquement difficiles. Il fait valoir que la lumière elle-même mettrait environ cinq ans pour effectuer un aller-retour jusqu'à l'étoile la plus proche, ajoutant que la galaxie spirale la plus proche de la Voie lactée (Andromède, l'une des « nébuleuses spirales » comme il les appelle) est plusieurs centaines de milliers de fois plus distante que les étoiles les plus proches.

L'essai se conclut avec enthousiasme : « avec des centaines de milliers de nébuleuses, contenant chacune des milliers de millions de soleils, la probabilité est énorme qu'il y ait un nombre immense de planètes dont les circonstances ne rendraient pas la vie impossible. » Churchill montre ici qu'il est familier des recherches de l'astronome Edwin Hubble à la fin des années 1920 et au début des années 1930, qui a découvert qu'il y a de nombreuses galaxies au-delà de la Voie lactée (environ 2000 milliards selon une estimation récente).

Mais sur une note plus sombre qui est le reflet de son époque, Churchill ajoute : « En ce qui me concerne en tout cas, je ne suis pas impressionné par les succès de notre civilisation au point d'être prêt à penser que nous sommes le seul endroit de ce vaste univers qui contienne des créatures vivantes et pensantes, ni que nous représentions le plus haut degré de développement mental et physique à être

jamais apparu dans l'immensité de l'espace et du temps. »

Près de quatre-vingts ans plus tard, la question qui obsédait Churchill est l'un des sujets de recherche les plus brûlants. La recherche de signes d'une vie souterraine sur Mars est en cours. Les simulations du climat de Vénus suggèrent qu'il n'est pas complètement impossible qu'elle ait été autrefois habitable. Les astronomes pensent que, dans quelques décennies, nous découvrirons des signatures biologiques de la vie passée ou présente dans les atmosphères de planètes extrasolaires, ou au moins que nous serons en mesure de donner des limites sur sa rareté.

L'essai de Churchill témoigne de sa vision selon laquelle les fruits de la science et de la technologie sont essentiels au développement de la société. Quand il contribua à la fondation du Churchill College à l'université de Cambridge, au Royaume-Uni, en 1958, il écrivit : « C'est seulement en menant l'humanité à la découverte de nouveaux champs de la science et de l'ingénierie que nous maintiendrons notre position et que nous continuerons à gagner notre vie. »

Une vision humaniste de la science

Mais il craignait également que sans la compréhension des humanités, les scientifiques n'opèrent dans un vide moral. « Nous avons besoin de scientifiques dans le monde, mais pas d'un monde de scientifiques », déclara-t-il. Afin que la science soit là « pour servir l'homme et non pour le gouverner », il pensait qu'il faut mettre en place des mesures politiques appropriées, inspirées par les valeurs humanistes. Comme il le dit dans un discours prononcé en 1949 à une assemblée de l'Institut de technologie du Massachusetts : « Si, avec toutes les ressources de la science moderne, nous nous trouvons incapables d'éviter une famine mondiale, nous serons tous responsables. »

Churchill était un fervent partisan de la science, mais il plaçait aussi les questions scientifiques importantes dans le contexte des valeurs humaines. Plus que jamais dans le paysage politique d'aujourd'hui, les dirigeants élus devraient s'inspirer de l'exemple de Churchill : nommer des conseillers scientifiques permanents, et en faire bon usage. ■

Cet article a été publié initialement par *Nature* le 16 février 2017 sous le titre *Winston Churchill's essay on alien life found* (<http://go.nature.com/2lkoXID>). La traduction et son édition a été réalisée par *Pour la Science*.

■ BIBLIOGRAPHIE

M. Livio et J. Silk, *Where are they ?*, *Physics Today*, à paraître.

C. Conselice *et al.*, *The evolution of galaxy number density at $z < 8$ and its implications*, *Astrophys. J.*, vol. 830, p. 83, 2016.

R. V. Jones, dans *Churchill* (éd. R. Blake et W. R. Louis), p. 437, Clarendon Press, 1996.

J. C. Humes, *Churchill : The Prophetic Statesman*, p. 82, Regnery History, 2012.

W. Churchill, *Churchill College*, *The New Scientist*, 15 mai 1958.

W. Churchill, *Fifty years hence*, *The Strand Magazine*, décembre 1931.



Abonnez-vous à

POUR LA
SCIENCE

OFFRE DÉCOUVERTE
12 n^{os} par an
4,90€
PAR MOIS
SEULEMENT

BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à : Pour la Science - Service abonnements - 19 rue de l'industrie - BP 90 053 - 67 402 Illkirch cedex

☒ **OUI**, je m'abonne à **Pour la Science** formule Découverte.
Je règle par prélèvement automatique de 4,90€ par mois et
je complète l'autorisation ci-contre. **J'économise 24% par mois.**
(DPV4E90)

MES COORDONNÉES

Nom : _____
Prénom : _____
Adresse : _____

Code postal _____

Ville : _____

Tél. Pour le suivi client (facultatif) : _____

E-mail obligatoire : _____

@ _____

J'accepte de recevoir les informations de *Pour la Science* ☐ OUI ☐ NON
et de ses partenaires ☐ OUI ☐ NON

Délai de livraison: dans le mois suivant l'enregistrement de votre règlement. Offre réservée aux nouveaux abonnés, valable jusqu'au 31/07/2017 en France métropolitaine uniquement. Pour un abonnement à l'étranger, merci de consulter notre site www.pourlascience.fr. Conformément à la loi "Informatique et libertés" du 6 janvier 1978, vous disposez d'un droit d'accès et de rectification aux données vous concernant en adressant un courrier à *Pour la Science*. Votre abonnement en prélèvement est reconduit automatiquement et peut être interrompu par simple lettre.

MANDAT DE PRÉLÈVEMENT SEPA En signant ce mandat SEPA, j'autorise Pour la Science à transmettre des instructions à ma banque pour le prélèvement de mon abonnement dès réception de mon bulletin. Je bénéficie d'un droit de rétractation dans la limite de 8 semaines suivant le premier prélèvement. Plus d'informations auprès de mon établissement bancaire.

TYPE DE PAIEMENT : PAIEMENT RÉCURRENT

Titulaire du compte

Nom : _____

Adresse : _____

Code postal _____ Ville : _____

Désignation du compte à débiter

BIC (Identification internationale de la banque) _____

IBAN _____
(Numéro d'identification international du compte bancaire)

Établissement teneur du compte

Nom : _____

Adresse : _____

Code postal _____ Ville : _____

Date et signature

Organisme Créancier

Pour la Science - 8 rue Férou - 75006 Paris

N° ICS FR92ZZZ426900

N° de référence unique de mandat (RUM)

Joindre un RIB

Partie réservée au service abonnement. Ne rien inscrire

LOGIQUE & CALCUL

Big Brother à nos portes (dérobées)

Parfois totalement indétectables, les portes dérobées informatiques nuisent gravement à la sécurité. Introduites à des fins d'espionnage ou de malveillance, ces « backdoors » exposent aussi chacun de nous au risque d'intrusion dans sa vie privée.

Jean-Paul DELAHAYE

Je ne veux pas vivre dans un monde où tout ce que je dis, tout ce que je fais, chaque personne à qui je parle, chaque expression de créativité, d'amour ou d'amitié, est enregistré.

Edward Snowden

En informatique et particulièrement dans tout ce qui est lié à la sécurité des systèmes, le terme de *backdoor* (signifiant « porte dérobée » ou « entrée cachée ») désigne un point d'accès secret. Celui-ci, ménagé dans un dispositif informatique, un programme, une machine, un réseau, permet d'en prendre le contrôle, d'en fausser l'usage ou au moins d'être informé de ce qui s'y passe, à l'insu de ceux qui s'en servent.

En cryptographie, ces portes dérobées donnent le pouvoir à celui qui en connaît l'existence de lire les messages chiffrés par un algorithme dont les utilisateurs pensent, de manière illusoire, qu'ils sont impossibles à percer. On a parfois envisagé d'installer des portes dérobées dont la présence serait connue de tous, mais dont l'accès serait réservé aux autorités.

Dans le cas d'un serveur reliant des machines ou constituant les nœuds principaux dans un réseau informatique, il s'agira de procédures permettant de contrôler les machines. Il s'agira aussi de dispositifs matériels mis en place dès la conception des machines, ou à l'insu de leurs fabricants après la sortie d'usine, et qui dupliquent

toutes les informations qui y passent et en envoient la copie à un destinataire complice, sans que le vendeur du matériel ou ses acheteurs ne le sachent.

Parfois, une porte dérobée est une fonction utilisée normalement lors de la mise au point des dispositifs logiciels ou matériels qui permet de les observer afin de comprendre ce qui s'y passe et corriger des erreurs éventuelles ; mais il arrive qu'on oublie de la supprimer ou de la désactiver avant la commercialisation, donnant ainsi la possibilité aux concepteurs des programmes d'y accéder subrepticement. La plus fameuse histoire de ce type concerne le poker en ligne.

Poker en ligne frauduleux

Cette porte dérobée fit gagner des millions de dollars à une équipe de tricheurs qui ne fut jamais parfaitement identifiée. Le principe de la tricherie était élémentaire : les développeurs d'un logiciel de jeu de poker en ligne avaient prévu une combinaison de touches qui leur donnait accès aux cartes cachées des adversaires, y compris quand ils n'étaient liés au système que comme simples joueurs et non comme administrateurs. Une fois le logiciel vendu et installé sur une plateforme qui n'était pas informée du trucage, ils s'inscrivaient comme simples clients et, lorsque les enjeux leur semblaient en valoir la peine, ils activaient la fonction qui leur montrait toutes les cartes, ce qui augmentait considérablement leurs chances de gagner !

L'escroquerie a duré des années, aux dépens d'une multitude de clients américains des sites *Ultimate bet* et *Absolute Poker* qui utilisaient, sans le savoir, le programme truqué. Russ Hamilton et plusieurs de ses complices ont ainsi gagné des sommes considérables entre 2003 et 2007. Ils se présentaient sous des identités différentes pour jouer, mais des experts attentifs qui étudiaient les taux de réussite des joueurs ont observé que certains comptes réussissaient souvent des coups qu'ils n'auraient dû gagner que rarement. Nionio, le premier joueur repéré, obtenait un taux de réussite 20 fois supérieur, pour certaines positions de jeu, à celui des meilleurs joueurs de poker.

Les sites de jeux, obligés de reconnaître les anomalies et donc la tricherie, ont dû rembourser partiellement les joueurs roulés. Ce qui a d'ailleurs mis en péril leur équilibre financier. Dans cette histoire, les escrocs et leurs complices ont gardé l'essentiel des sommes acquises. Des études détaillées des parties jouées au cours de la période concernée indiquent que plus de 110 noms de joueurs fictifs avaient tiré des gains anormaux du jeu. Le montant des sommes volées grâce à la porte dérobée a été évalué à plus de 22 millions de dollars.

Lors du développement d'un logiciel, il est nécessaire de disposer de fonctions d'observation qui donnent des droits supérieurs à ceux des utilisateurs normaux. Cela facilite la maintenance, le repérage des