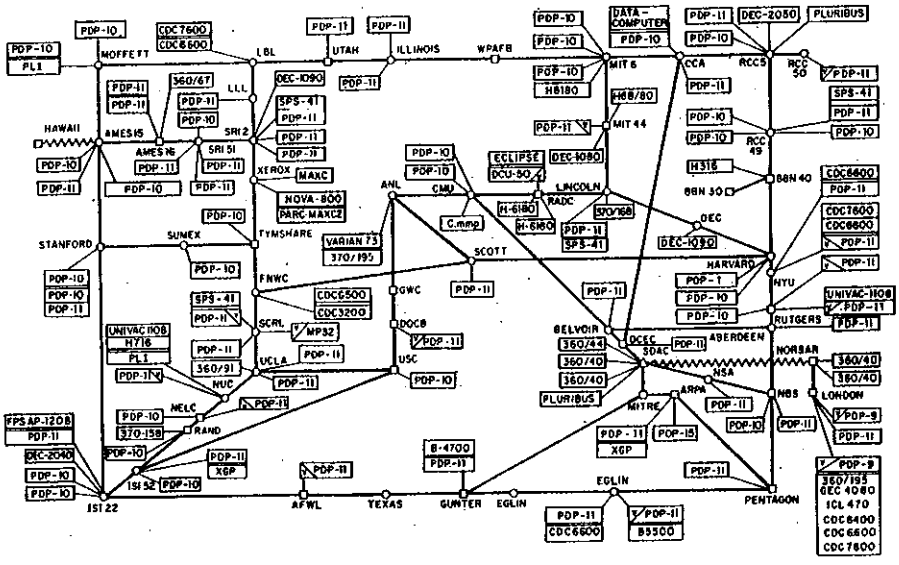
Le monde a ses **réseaux**...

En 40 ans, les réseaux, et en premier lieu Internet, ont conquis le monde et l'ont transformé. Nous sommes désormais dans une société de l'information où bénéfices et inconvénients vont de pair. L'exploration des rouages des réseaux de communication n'en est que plus indispensable.

Les technologies et les infrastructures de communication ont été au cœur de nombreux enjeux dans toutes les civilisations. Mais le passage au numérique a constitué une rupture qualitative et un changement d'échelle drastique. Aujourd'hui, les enjeux économiques et sociaux des réseaux de communication concernent tous les secteurs d'activité, de la production de biens et de services, à la santé et à la sécurité. Ils contribuent de façon essentielle à l'accélération des progrès scientifiques et techniques, aux gains de productivité et à la croissance.

L'économie, au sens large de l'ensemble des échanges entre les hommes, et la société tout entière, sont bouleversées par les nouvelles infrastructures et modalités offertes pour communiquer, interagir et produire. Internet est l'incarnation de ces nouvelles infrastructures de communication numérique. Internet, qui soufflera bientôt ses 40 bougies, s'est progressivement imposé comme moyen de communication privilégié, parfois au détriment d'autres médias, tels la presse et l'audiovisuel.

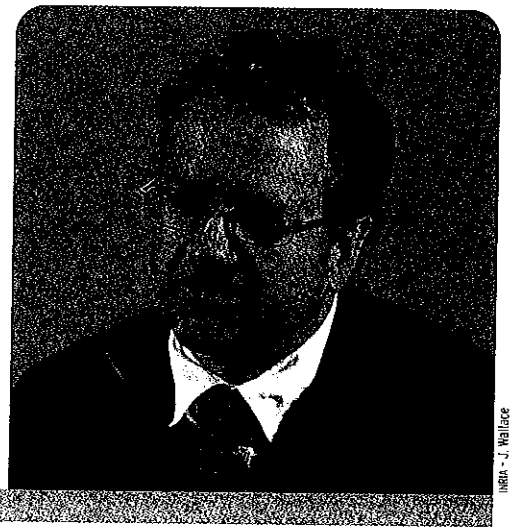
Cependant, si cette nouvelle façon de communiquer présente bien des opportunités, elle n'est pas exempte de dangers, notamment lorsqu'elle n'est pas bien comprise et maîtrisée. Afin de mieux cerner les problèmes et les défis auxquels sont confrontés les chercheurs qui travaillent sur les réseaux, sur la communication ainsi que sur l'accès à l'information, replaçons les développements et les évolutions de ce domaine dans une perspective historique. Pour ce faire, nous dissocierons trois aspects liés à l'« écosystème Internet » : les réseaux, les outils de communication et ceux pour accéder à l'information.



L'ANCÊTRE D'INTERNET, ARPANET, reliait une centaine de laboratoires américains en 1977.

Un développement fulgurant

Le réseau ARPANET, l'ancêtre d'Internet, n'était constitué, en 1970, que de quatre machines connectées, toutes installées dans des laboratoires d'universités américaines. Sept ans plus tard, seulement 100 machines étaient reliées, toujours hébergées par des laboratoires de recherches *(voir la figure ci-contre)*. Puis le nombre de machines s'est accru exponentiellement *(voir la figure, page ci-contre)* : 200 000 machines en 1987, 20 millions en 1997, 500 millions en 2007 et on parle aujourd'hui d'environ deux milliards de dispositifs connectés à Internet. Cette croissance résulte notamment de l'engouement pour les téléphones portables, tels les *smartphones* (des téléphones intelligents, tel l'iPhone d'*Apple*) dotés de toutes les fonctionnalités pour



de Thierry PRIOL
Directeur scientifique adjoint à l'Institut national de recherche en informatique et en automatique (INRIA)

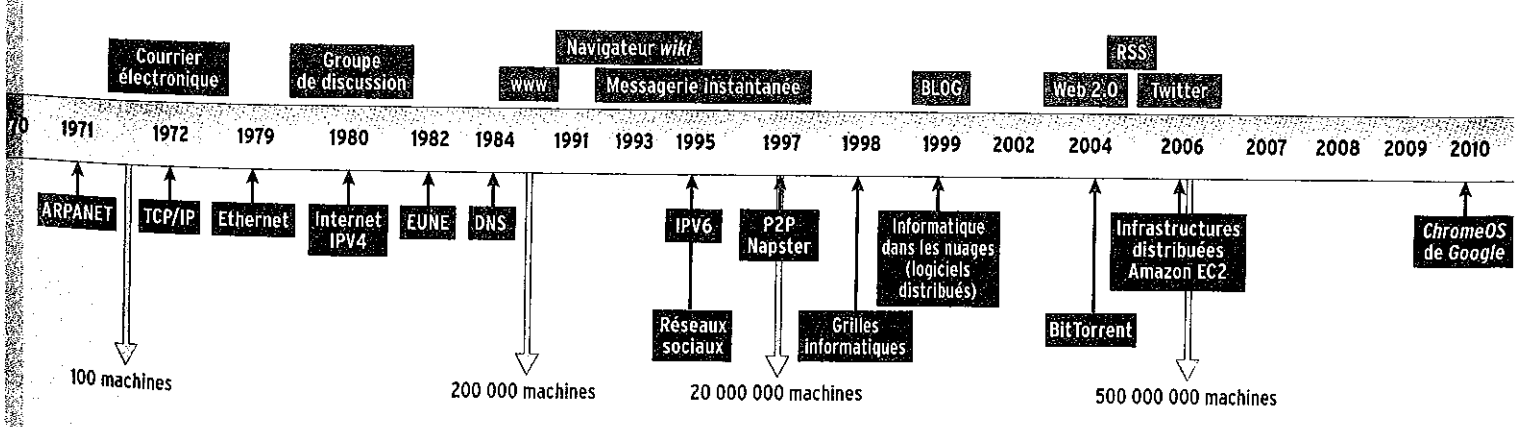
accéder à Internet. Ce nombre risque encore d'augmenter avec l'Internet des objets permettant de connecter et d'identifier un nombre considérable d'artefacts des plus banals de la vie quotidienne (voir *Les objets en réseau*, par D. Simplot-Ryl, page 34).

La poussière intelligente

Avec l'arrivée des nanotechnologies, certains parlent même de « poussières intelligentes », des petits dispositifs autonomes, de dimension millimétrique, voire inférieure, dotés de capteurs, de capacités de calcul et de communication sans fil. Ces dispositifs vont gonfler le nombre d'entités connectées à Internet. Or chaque machine connectée à Internet doit disposer d'un numéro, un numéro IP... Le risque de pénurie de numéro est proche, car le système en vigueur ne prévoit que quatre milliards de ces numéros. Toutefois, ingénieurs et chercheurs avaient prédit cette situation et ont proposé des modifications du protocole IP, le langage de communication universel d'Internet, en proposant IPV6 en 1995. Ce système autoriserait plus de 10^{38} machines à se connecter à Internet, mais son déploiement tarde à se réaliser.

Ce changement dans la taille et dans la complexité des infrastructures de communication suscite des débats au sein de la communauté Internet : les choix de conception et les hypothèses prises il y a 40 ans sont-ils encore valides aujourd'hui ? Les faiblesses structurelles d'Internet sont connues notamment dans le domaine de la sécurité, de la qualité de service, de la mobilité, du temps réel et du nommage. Citons aussi le problème des protocoles de communication qui ne sont pas encore capables de prendre en compte les contraintes des applications en termes de bande passante, ceux des délais et des fortes variations durant la transmission ainsi que celui de la fiabilité.

Aujourd'hui, le nommage, c'est-à-dire la façon d'identifier un site ou une donnée que l'on souhaite consulter, dépend de la localisation physique de la machine où se trouve l'élément désiré, ce qui entraîne souvent des erreurs lorsque, par exemple, une machine n'existe plus ou a changé de nom (voir *L'architecture*



40 ANS D'HISTOIRE des réseaux, en quelques événements clefs.

d'Internet à l'ère du mouvement, par W. Dabbous, page 26). Dans le futur, Internet dissociera sans doute réseaux physiques et réseaux virtuels et seuls ces derniers seront accessibles à l'utilisateur.

Pour faire évoluer Internet et résoudre les problèmes précédents, des efforts importants de recherche académique et industrielle ont été entrepris, illustrés par de grandes initiatives internationales. Citons GENI *(Global Environment for Network Innovations)* de la NSF (l'Agence américaine de financement de la recherche) et celle de la Commission européenne (FIRE, pour *Future Internet Research and Experimentation*). Deux écoles s'affrontent : faut-il améliorer l'existant en y apportant des modifications étape par étape ou bien faut-il refonder Internet pour corriger ses faiblesses en développant une nouvelle infrastructure ? Le débat est ouvert et est loin d'être clos.

De l'utilité des mathématiques

Quelle que soit l'approche suivie pour faire évoluer Internet, il sera nécessaire de mieux comprendre son fonctionnement ainsi que ses performances, ceci afin de pouvoir le dimensionner correctement. Compte tenu de la taille du réseau, du caractère aléatoire des accès à celui-ci, le problème est devenu extrêmement difficile et une réponse purement technologique n'est sans doute pas la plus appropriée. Les mathématiques fournissent de bien meilleurs outils et notamment l'utilisation de la théorie des probabilités. Grâce à elle, on peut représenter mathématiquement l'état d'un réseau et répondre à des questions liées au dimensionnement des réseaux (voir *1909-2009, l'odyssée des réseaux*, par Ph. Robert, page 42).

Les mathématiques aident aussi en dégageant des lois fondamentales qui régissent les réseaux. On a ainsi montré que la construction du réseau Internet n'est pas complètement aléatoire, mais qu'il est constitué de supernœuds (voir *Les réseaux invariants d'échelle*, par A.-L. Barabási et É. Bonabeau, page 50). C'est un réseau invariant d'échelle doté de propriétés intéressantes quant à la fiabilité (la disparition d'un nœud ne remet pas en cause son fonctionnement) et à la sécurité (l'organisation d'Internet favorise la propagation des virus).

Un autre aspect important concerne la gouvernance de l'infrastructure. Plusieurs acteurs y sont impliqués et ceux-ci doivent se coordonner sur plusieurs plans : la définition des standards, l'attribution des noms de domaine et la législation dans un contexte international (voir *Comment gouverner Internet ?*, par J.-F. Abramatic, page 116). L'enjeu est de conserver l'espace de créativité qui a fait le succès d'Internet tel que nous le connaissons aujourd'hui.

L'infrastructure du réseau Internet n'est qu'un moyen de transporter des données d'une machine à une autre. Pour s'abstraire de cette infrastructure et proposer des outils de communication de plus haut niveau, des protocoles et des applications de plus en plus élaborés ont été conçus afin de faciliter l'échange d'informations entre utilisateurs.

Ainsi la communication par courrier électronique est apparue dès le début des années 1970 avec notamment la possibilité d'identifier un utilisateur sous forme d'une adresse unique combinant le nom de la machine qui recevra le courrier et celui de l'utilisateur sur cette machine : c'est l'adresse que nous connaissons et qui contient l'arobase @. Le courrier électronique a été rapidement adopté dans le cadre privé, mais aussi comme outils d'échange d'informations au sein des entreprises en favorisant une interaction décalée entre les utilisateurs, à l'inverse du téléphone ou de réunions.

Le courrier électronique est devenu indispensable dans une économie mondialisée, mais il est aussi devenu un vecteur de virus, de messages non sollicités (les « spams ») et un moyen d'usurper une identité et de récupérer des informations confidentielles (voir *Boulevard du cybercrime*, par J.-Y. Marion et M. Kaczmarek, page 78). C'est aussi un moyen de communication très peu sécurisé, car l'échange de courriers n'est souvent pas crypté. On peut également s'interroger sur la

LE LHC DU CERN produira d'énormes quantités de données qui seront traitées sur des grilles de calcul, c'est-à-dire des ordinateurs et des serveurs répartis dans le monde et reliés par Internet.

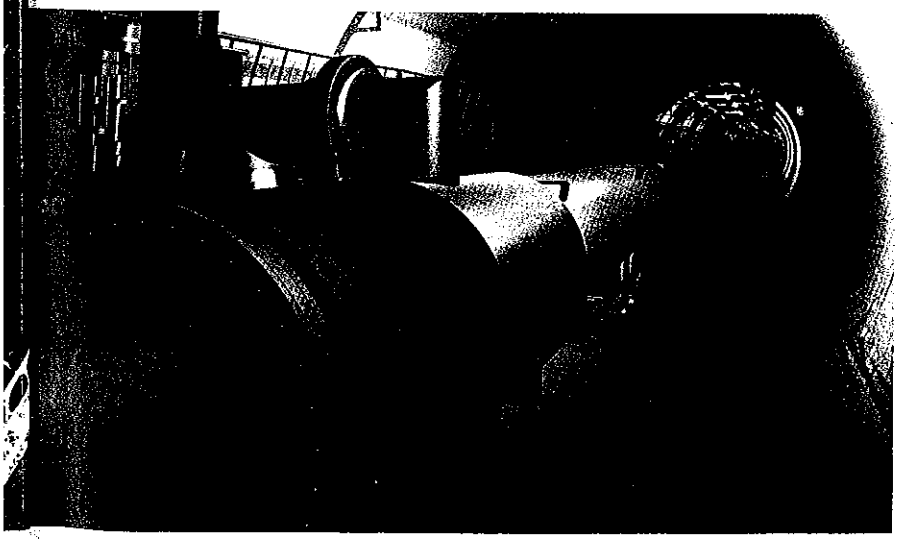
pertinence de l'instantanéité des échanges de courriers : on se débarrasse souvent d'un problème en envoyant un message à un collègue alors qu'on aurait pu le résoudre soi-même.

Le besoin de communiquer

L'échange de courriers s'est vite révélé insuffisant, car il permet difficilement de communiquer au sein d'une communauté s'organisant dynamiquement autour d'un sujet d'intérêt commun. Dès les années 1980, les premiers groupes de discussion sont apparus sur le réseau USENET et sont toujours en usage malgré l'apparition d'outils plus élaborés (forum ou blog). Dans ces groupes de discussion dédiés à un sujet donné, les utilisateurs envoient des contributions qui seront lues par les utilisateurs abonnés au groupe. Chaque utilisateur est connecté à un serveur de groupe de discussion et ce sont les serveurs qui échangent les contributions. La communication n'est donc pas immédiate, car la contribution doit se propager d'un serveur à l'autre.

Au milieu des années 1990, est apparu un nouveau mode de communication, fondé sur le concept de réseau social, qui prend en compte les liens (familiaux, professionnels, amicaux...) tissés entre les individus. Ainsi, chacun peut se créer un réseau sur lequel il partage des informations : parcours scolaire et professionnel, carnet d'adresses, fichiers multimédia (musique, images, vidéo...). Aujourd'hui, les applications utilisées pour développer des réseaux sociaux jouissent d'une grande popularité, mais elles ne sont pas sans danger.

En effet, n'importe qui peut collecter des informations sur un individu et en faire un usage qui va parfois contre l'intérêt de celui-ci. Pire, il est difficile, voire impossible, d'effacer le contenu de ses communications, le droit à l'oubli est aujourd'hui impossible sur Internet. La prudence est donc de rigueur quand on expose sa vie privée au risque un jour d'avoir des conséquences inattendues (voir *Internet et vie privée : des frères ennemis ?*, par Cl. Castelluccia, page 92).



Que serait Internet sans le Web ? Issu des travaux de Tim Berners-Lee au CERN au début des années 1990, mais aussi des recherches sur l'hypertexte (des documents sont reliés entre eux par des « hyperliens » grâce auxquels on passe de l'un à l'autre), le Web est devenu l'outil incontournable pour accéder à une masse d'information considérable. En 20 ans, il a bouleversé nos modes d'accès à l'information.

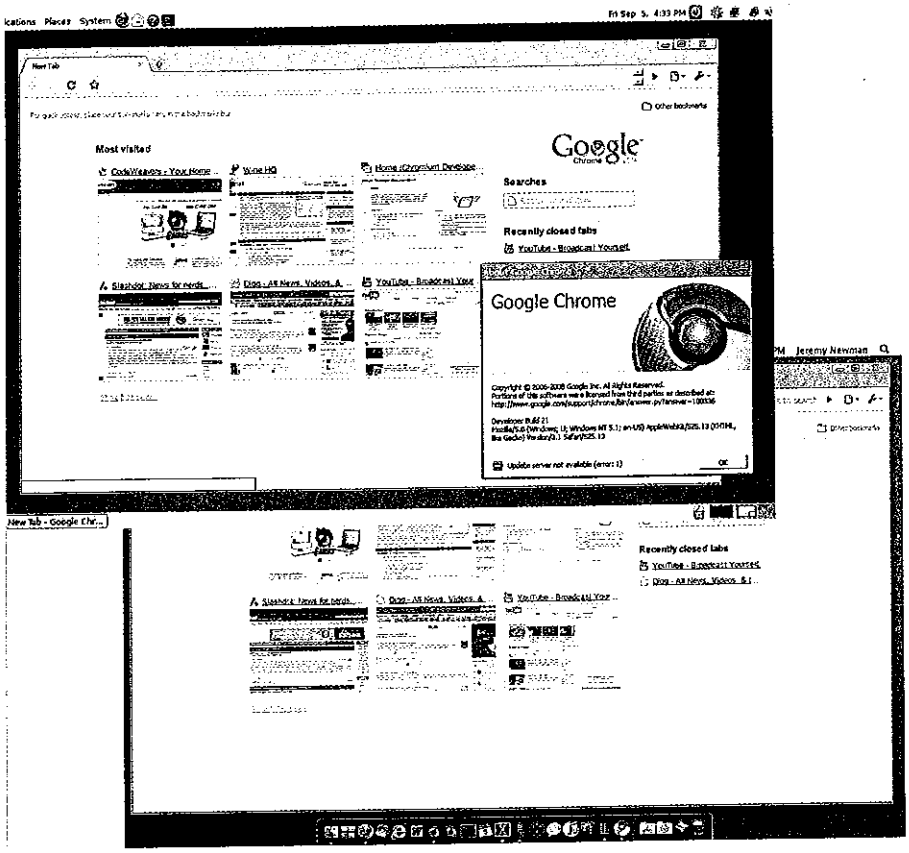
La démesure du Web

Aujourd'hui, on répertorie environ 240 millions de sites Web à travers le monde. Comment trouver une information pertinente dans cet océan ? Grâce aux moteurs de recherche, devenus indispensables pour trouver une information à partir de mots-clés. Les premiers sont mis au point quelques années après la naissance du Web : *Yahoo* en 1994, *Altavista* en 1996 et enfin, *Google* en 1998. Le succès de ce dernier tient à sa façon d'indexer les pages, mais aussi à son modèle économique. Il a révolutionné les moteurs de recherche en introduisant l'idée de popularité d'une page Web, c'est-à-dire le nombre de fois où celle-ci est référencée par un site Web. Plus cette popularité est grande, plus son rang d'apparition dans les résultats est élevé (voir *Le secret de* Google, par J.-P. Delahaye, page 64).

Mais aujourd'hui l'information n'est plus seulement textuelle. Le Web héberge de plus en plus de données multimédia : musique, images et vidéo. De nouveaux moteurs de recherche sont à inventer avec des méthodes d'indexation inédites pour classer les données multimédia et les restituer aux internautes (voir *Naviguer dans l'océan du multimédia*, par N. Boujemaa, page 70). L'enjeu est de transformer le Web en un service pour accéder à la connaissance, ce qui soulève de nombreux problèmes pour la maîtrise d'un volume considérable de données hétérogènes et pour le développement de nouvelles fonctionnalités portant sur les contenus des données et répondant à des besoins de haut niveau d'utilisateurs individuels et de communautés.

Le Web était au départ un média de communication statique où les informations étaient mises à disposition des utilisateurs par les gestionnaires des sites Web. Il s'est transformé en un média plus dynamique où interagissent rédacteurs et lecteurs d'information. Cette évolution, connue sous le terme Web 2.0, a donné naissance à un ensemble de techniques, tels les blogs ou les wikis, autorisant le lecteur à corriger et à commenter les informations. L'exemple le plus connu est *Wikipédia*, une encyclopédie qui s'est construite à partir de contributions collectives *via* le Web.

Cependant, le Web n'est pas seulement un vaste espace d'informations librement accessibles.



LE SYSTÈME D'EXPLOITATION *Chromeos*, élaboré par *Google*, est fondé sur l'informatique dans les nuages : informations et logiciels sont situés dans des centres de stockage auxquels on accède par Internet.

Des informations doivent parfois être protégées du regard des autres et réservées à un nombre restreint d'individus. Ces restrictions valent à la fois pour les informations transmises sur des réseaux filaires et plus encore sur les réseaux sans fil où n'importe qui peut capter les ondes émises par les bornes Wi-Fi. Là aussi les mathématiques sont une aide précieuse, car il faut sans cesse inventer de nouvelles techniques de protection des données.

Aujourd'hui, la confidentialité des communications est assurée par un protocole cryptographique, nommé RSA, inventé à la fin des années 1970 et fondé sur la difficulté à factoriser des grands nombres (voir *Les courbes, garantes de la sécurité*, par P. Gaudry, page 56). Pourtant, en 1999, une équipe a réussi à casser le protocole RSA fondé sur une clé de 512 bits en utilisant près de 300 machines fonctionnant en parallèle, ce qui représente l'équivalent d'environ 38 ans de calcul sur un processeur unique. Certes, décrypter de la sorte un message n'est pas à la portée de tout le monde, mais des organisations gouvernementales peuvent réunir les compétences nécessaires et les utiliser à des fins d'intelligence économique. La présence de supercalculateurs au sein de la NSA, l'Agence de sécurité des États-Unis, ne doit donc pas étonner !

Pour les réseaux sans fil, la situation est plus inquiétante : l'utilisation de 20 ordinateurs personnels équipés de cartes graphiques puissantes, et dont les processeurs ont été détournés de leur fonction pour faire du calcul, a permis de casser le protocole WPA utilisé pour protéger les bornes Wi-Fi et réputé plus sûr que le protocole WEP habituellement employé dans les réseaux filaires.

livres

- C. HUITEMA, *Et Dieu créa l'Internet*, Eyrolles, 1995.
- E. KROL, *Le monde Internet*, O'Reilly International, 1995.

internet

- http://news.netcraft.com/archives/web_server_survey.html
- GENI : http://www.geni.net
- FIRE : http://cordis.europa.eu/fp7/ict/fire/
- http://interstices.info/jcms/c_41560/les-debuts-du-web-sous-lil-du-w3c?hlText=Internet

Les bornes Wi-Fi seraient le point faible d'Internet, car elles autorisent n'importe qui à utiliser l'accès Internet d'un particulier pour, par exemple, des téléchargements illicites, mettant ainsi le propriétaire français de la borne Wi-Fi sous le coup de la récente loi *Création et Internet*, la loi dite Hadopi (voir *La loi Hadopi est-elle applicable ?*, entretien avec Cl. Kirchner, page 106). De nouvelles techniques de cryptage, comme celles fondées sur les courbes elliptiques, encore plus difficiles à casser sont donc nécessaires.

Toutefois, on doit concilier deux impératifs : rendre difficile, voire impossible, le décryptage, mais avec des techniques qui nécessitent peu de calcul à la fois pour le cryptage et pour le décryptage, car dans l'avenir le terminal d'accès à Internet sera majoritairement un dispositif mobile dont la consommation énergétique est contrainte pour des raisons d'autonomie.

Calculer sur Internet

L'accroissement des performances des réseaux a fait naître un nouvel usage : on peut désormais calculer sur Internet en le transformant en un vaste supercalculateur. C'est ce qu'autorisent les grilles informatiques *(voir la figure, page 6)*, qui apparaissent à la fin des années 1990, suivies au milieu des années 2000 de l'idée d'informatique dans les nuages : le stockage et le traitement des données sont assurés par des serveurs éloignés auxquels on accède par Internet (voir *Vers le tout-en-réseau ?*, par Th. Priol, page 16). Cette disparition du rôle central de l'ordinateur individuel, beaucoup d'applications migrant vers les serveurs, est associée aux grands centres de données qui sont maintenant incontournables. On est sans doute à la veille d'une révolution, qui changera la méthode d'accès aux logiciels qui seront accessibles *via* le réseau et non plus installés sur la machine de l'utilisateur.

Dans ce contexte, l'arrivée du nouveau système d'exploitation *ChromeOS* n'est pas surprenante : il n'a pas été élaboré par *Microsoft*, l'inventeur de *Windows* et maître du logiciel, mais par *Google*, le roi d'Internet ! *ChromeOS* est d'une simplicité déconcertante : il s'agit essentiellement d'un logiciel de navigation sur le Web *(voir la figure ci-dessus)* qui donne accès à un espace virtuel où l'on accède aux données et aux applications délocalisées !

Là encore, cette évolution ouvre de nouveaux usages, mais fait aussi naître de nouveaux risques… Internet ne risque-t-il pas d'être contrôlé par ceux qui disposent des infrastructures de traitement de l'information ? Internet menace-t-il la démocratie ou la renforce-t-il ? Restons optimistes, Internet sera ce que les citoyens en feront, à condition que chacun comprenne bien les évolutions, les enjeux et les risques.