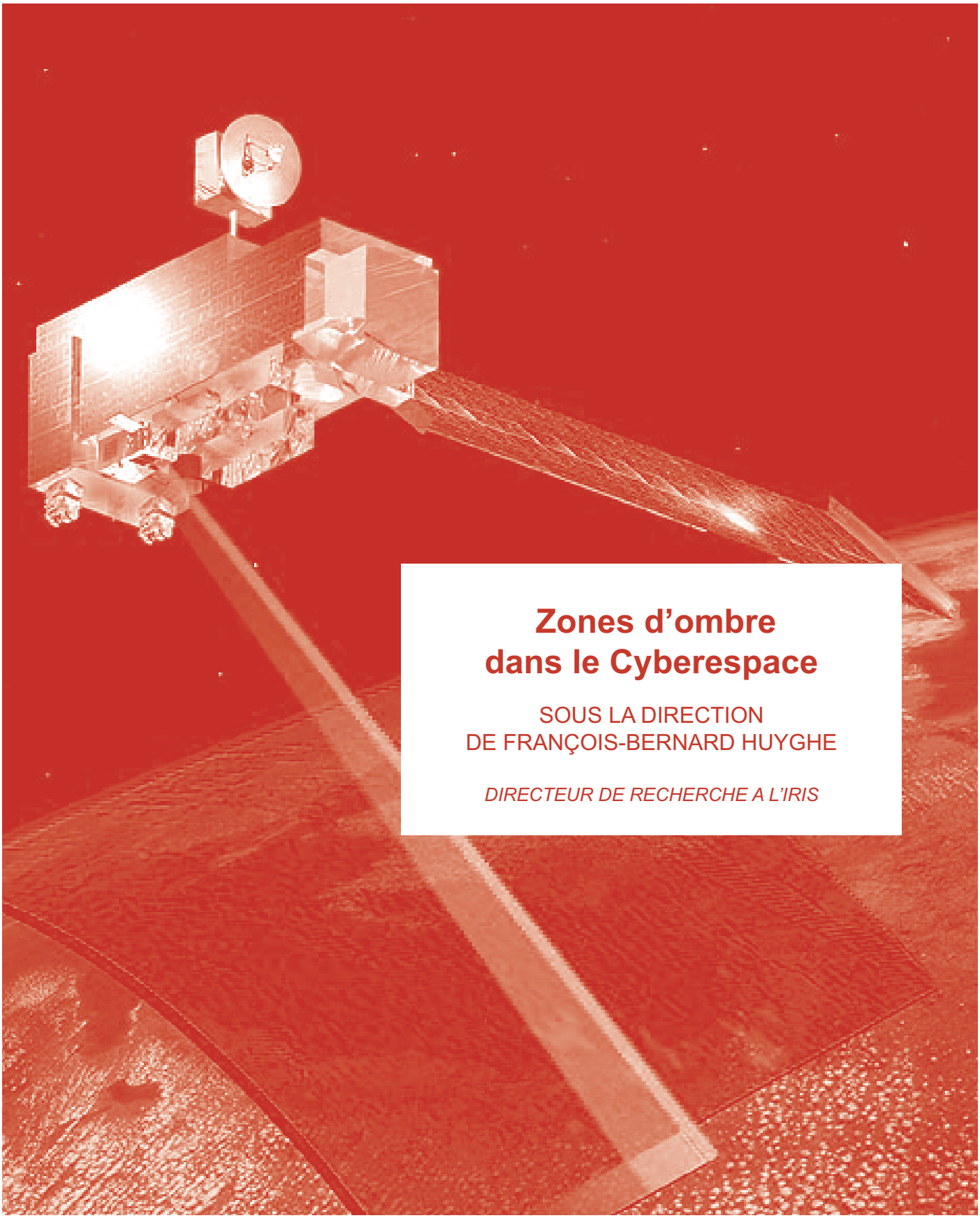
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION

octobre 2013



Zones d'ombre dans le Cyberespace

SOUS LA DIRECTION
DE FRANÇOIS-BERNARD HUYGHE

DIRECTEUR DE RECHERCHE A L'IRIS

Internet, entre ombre et lumière

Il est rare qu'il soit question d'Internet sans voir évoquer deux images opposées. Soit une source où toutes les informations sont disponibles : la transparence progresse ; l'internaute peut dire et partager pour le plus grand bénéfice de la démocratie. Soit l'image d'un monde occulte, truqué et où Big Brother (Prism ou une de ses variantes) surveille tout dans l'ombre. Le propos de ce numéro est plutôt de nous interroger sur ce qui fait du virtuel un objet aussi ambigu. S'il y a des choses cachées depuis la fondation du Net, cela tient-il seulement au bon ou au mauvais usage que nous en faisons, nous ou nos gouvernants ?

Kavé Salamatian explique dans un premier temps comment les trois « couches » d'Internet (matérielle avec les terminaux et vecteurs, logicielle avec les protocoles, les normes et tout ce qui régule les échanges, sémantique avec le contenu des messages qui s'échangent) sont intrinsèquement génératrices de conflits et de contradictions. Maxime Pinard nous montre ensuite qu'à rebours du discours qui décrit les frontières comme condamnées à l'ère numérique, le cyberespace pourrait bien être en voie de balkanisation.

Daniel Ventre analyse, de son côté, comment se développe au sein d'Internet un territoire autonome et sécurisé : celui de TOR, un espace privé inclus dans l'espace commun. Enfin, Philippe Blanc revient sur le protocole Bitcoin. Il analyse comment un des principaux privilège de l'État souverain : celui de battre monnaie, ou du moins de produire des moyens de paiement, est remis en cause par un logiciel.

Nous aurions sans doute pu poursuivre la liste : comment il se fait qu'il existe un web invisible inaccessible aux moteurs de recherche ? Qui contrôle le système de routage et d'adressage des milliards de messages qui circulent sur la Toile ? Les fermes de données, les possibilités cachées des applications ? La part du vi-sible et de l'obscur dans le Cyberespace nous révèle en réalité de nouveaux rap-ports des pouvoirs politiques, économiques et techniques. ■

François-Bernard Huyghe

Le côté occulte de l'architecture d'Internet

par Kavé Salamatian,
Professeur d'informatique à l'université de Savoie

Internet est devenu le sujet de toutes les craintes. Il existerait un réseau souterrain, profond, qui serait un repère de personnes asociales et marginales, ces fameux ou infâmes « hackers ». Mais l'Internet serait aussi un terrain obscur où depuis de longues années une surveillance porterait atteinte à nos vies privées. On pourrait considérer que cette sensation est accentuée par la complexité d'Internet et le peu de connaissance qu'a le grand public de ses mécanismes internes. Mais l'Internet n'est pas le seul système complexe donc le commun des mortels ne connaît pas les détails. Le système ferroviaire, les avions, les centrales nucléaires... sont d'autres systèmes complexes mais qui ne sont pas soupçonnés d'abriter des bas-fonds.

Qu'est-ce qui explique le fait que l'Internet soit devenu un terrain de prédilection pour des groupes que certains peuvent considérer comme marginaux, comme les hackers, ou plus prosaïquement secret, comme la NSA entre autres ? Outre les raisons évidentes relatives à la place centrale qu'a prise ce réseau dans nos sociétés et à la large utilisation de celui-ci, il existe des causes plus fondamentales relatives à l'architecture de ce réseau que nous allons tenter de décrypter dans cet article.

De l'architecture de l'Internet

Il convient de se rappeler qu'une grande partie des concepts fondamentaux de l'Internet tel que nous le connaissons a été développée dans les années 1970 sur la côte Ouest des Etats-Unis à une époque où le courant libertaire était très fort. Ainsi de façon peut être inconsciente, les pères fondateurs de l'Internet ont introduit dès le début des principes de décentralisation et d'absence de contrôle dans l'architecture qui impactent encore aujourd'hui l'Internet. En effet, l'architecture de l'Internet est fondée sur un modèle en couches ; les fonctionnalités du réseau sont découpées en couches séparées ; ces couches n'interagissent qu'à des points bien précis par des échanges d'informations ; l'interaction n'est contrôlée que de façon locale en ne vérifiant que l'information pertinente à la couche recevant les données. Ainsi, du moment que le service rendu par chaque couche ne change pas, les couches peuvent être modifiées sans impacter les couches voisines. Ce modèle en couche qui a été normalisé par l'Organisation des Standard Internationaux (l'OSI) et l'Union Internationale des Télécommunications (UIT), est aussi utilisé par l'Internet qui s'est développé en dehors de son giron. Les normes de l'Internet sont développées par l'IETF (Internet Engineering Task Force), qui, à l'inverse de l'UIT qui est un organisme international dont les États et les grands opérateurs sont membres, est un forum ouvert à tous ceux qui ont la compétence technique et technologique.

L'architecture en couches a été un formidable atout pour l'Internet, car elle permet aux différents acteurs de travailler indépendamment les uns des autres ; ceux qui développent des applications n'ont pas à interagir directement avec ceux qui déploient les câbles ; l'arrivée d'un nouveau support de communication comme la 4G ne nécessite pas de changer toute l'architecture du réseau ou de réadapter les applications. C'est ce modèle qui explique largement la croissance exponentielle de l'Internet. Les acteurs des différents niveaux ont pu in-

■■■ -nover, développer et déployer leurs services en autarcie et ainsi créer de nouvelles fonctionnalités sur lesquelles les autres acteurs ont pu s'appuyer pour fournir de nouveaux services. L'exemple parfait de cette symbiose est fournie par le protocole « http » (Hyper Text Transfer Protocol) qui permet l'accès aux pages web. Ce protocole s'est construit au dessus et grâce à TCP/IP, qui lui même s'appuie sur les services fournis par les couches inférieures afin de transférer les paquets contenant le texte des pages web d'un point à l'autre du réseau et de choisir le chemin à suivre pour relier la source et la destination. Le développement du protocole http a ensuite permis la croissance d'un très riche écosystème que l'on appelle communément la toile ou le web. L'architecture en couches a été un tel succès qu'aujourd'hui certains croient que le web est l'Internet et en oublient les couches sous-jacentes.

Nous avons aussi pu lire ces derniers mois dans certains journaux que l'Internet avait 20 ans car c'était en avril 1993 que le CERN mit dans le domaine public ses travaux autour du « www » et publia la première page web accessible librement, alors qu'avant cette date il y avait déjà plus de 20 ans d'existence d'Internet. Nous verrons dans la suite que la myopie induite par l'architecture en couches est un problème essentiel qui explique largement la surprise qu'ont la plupart des personnes quand ils entendent parler des « bas-fonds » de l'Internet. Même si l'architecture en couches a été normalisée par l'UIT ainsi que par l'IETF, Il existe néanmoins certaines différences essentielles entre ces deux visions. Alors que la norme OSI distribue les fonctionnalités aux différentes couches et normalise ces fonctionnalités, l'IETF s'intéresse principalement à normaliser l'interface entre les couches. Ceci donne une très grande flexibilité à l'architecture IETF car elle permet d'interconnecter facilement tout composant suivant les recom--mandations de l'interface. Ceci est illustré parfaitement par l'interface des « sockets ». Cette interface permet à une application de communiquer avec le réseau, et ceci indépendamment du type de réseau sous-jacent, du type d'application, et même relativement du type de système d'exploitation, car cette interface existe à peu près avec la même structure dans tous les systèmes et sur toutes les plates-formes. Ainsi une application développée sur une plate-forme peut être rapidement transférée sur une autre plate-forme sans changement, du moins dans sa partie réseau. Dans la vision OSI, ce serait les fonctionnalités et les messages à échanger afin d'accéder à celle-ci qui serait normalisés et non pas l'interface logicielle, permettant ainsi à des fournisseurs de matériels d'assurer leurs marges en gardant captifs les clients utilisant leurs interfaces tout en fournissant des appareils à fonctionnalités comparables. Cette différence peut sembler anecdotique aujourd'hui où l'architecture Internet de l'IETF a largement vaincu toutes les approches concurrentes, mais dans les années 1980 et 1990 ce sujet a été un domaine de controverse essentiel dont on voit encore les soubresauts dans la tentative de l'UIT au WCIT de reprendre le contrôle des réseaux.

De l'impact de l'architecture

Nous avons vu que le modèle en couches, de par sa flexibilité, a été un formidable atout pour l'Internet, en lui permettant de très vite se développer et en favorisant l'émergence rapide de nouveaux services et de nouveaux paradigmes. C'est cette flexibilité qui permet aujourd'hui la pénétration rapide de l'Internet dans tous les aspects de notre vie. Il n'y a plus besoin comme dans les temps anciens pourtant si proches d'avoir un poste radio pour écouter la radio, un poste de télévision pour accéder à l'image et d'un fax ou d'un télex pour se transmettre des messages. Maintenant tout passe par une fenêtre unique : votre ordinateur, par une interface unique : votre navigateur et par un canal unique, l'Internet. Mais c'est aussi cette flexibilité qui permet aujourd'hui aux personnes se trouvant dans des pays où la censure règne de la court-circuiter et d'user de leur droit à avoir accès à une information libre. Mais c'est aussi cette même flexibilité qui permet à toute une ribambelle de ■■■

communautés de se cacher grâce à l'opacité qui existe entre les couches.

En effet l'architecture en couches n'est viable que si nous faisons confiance aux couches supérieures et inférieures, i.e., que nous soyons assurés que ces couches ne font que ce qu'elles sont censées faire et rien d'autre. Par exemple la couche IP n'est pas censée garantir que le chemin que prendra un paquet soit connu à l'avance. Si vous ne pouvez faire confiance au chemin choisi par votre opérateur il faudra que vous ajoutiez des couches qui vous protégerons des risques ou des impacts de l'opérateur. Le réseau n'est pas censé garantir votre anonymat. Si cela est important pour vous, il faudra vous prémunir de la divulgation de votre identité par la mise en place de mécanismes adéquat, par exemple un routage en oignon similaire à celui utilisé par le réseau TOR. De même, la couche physique n'est pas censée nous informer si le câble optique qu'elle emploie est instrumenté pour être écouté. En fait toute couche de l'architecture de par son opacité peut être, selon le point de vue, un risque, ou une opportunité, pour chaque acteur du réseau.

Cela explique très bien pourquoi nous avons parfois le sentiment que l'Internet est le repère de tous les bas-fonds et de tellement de choses cachées. Ses entrailles, de par l'architecture en couches, contiennent tellement de méandres et de lieu où il est facile de se cacher pour le bien ou pour le mal, qu'il est naturel que l'Internet soit un repère d'activités diverses et variées. Ce sont les choix architecturaux fondamentaux de l'Internet qui aboutissent à cet état de fait. L'Internet ne pourra être sécurisé sans changer fondamentalement et perdre une part de son âme libertaire. La surveillance ne pourra être interdite, car la flexibilité permettra toujours de trouver un recoin où elle pourra sévir. Mais d'un autre coté on pourra toujours contourner la surveillance en utilisant cette même flexibilité architecturale. Tout ceci est inscrit dans l'ADN de l'Internet. Ainsi les parties cachées de l'Internet sont intrinsèques à ce réseau et leur existence n'est nullement étonnante. Ce qui est par contre étonnant est notre surprise et notre attente que l'Internet soit un havre de paix où tout serait transparent.

Les questions fondamentales auxquelles nous sommes aujourd'hui confrontés sont les suivantes. Puisque cette confiance que nous espérions avoir vis-à-vis du réseau, et même plus généralement de chaque couche vis-à-vis des couches inférieures, semble inaccessible, est-il réellement nécessaire de l'atteindre au prix de son âme libertaire ? Et puisque le salut ne viendra pas à court terme de la technologie (puisque le problème est fondamental), ne faut il pas apprendre à vivre dans un monde où il y aura des risques de surveillance sur nos informations privées, des risques de cyber-délinquance, et des risques de cyber-guerres ? Ces questions peuvent sembler être des questions éminemment branchées et issues du XXIème siècle, mais à les regarder de façon plus précise nous voyons bien que ces questions sont des corollaires à des problèmes plus anciens qui ont traversé les civilisations humaines durant des millénaires. La première question est bien évidemment relative à la tension entre sécurité et liberté et la seconde repose la question de la primauté de l'éducation. Même si ces questions se reposent aujourd'hui avec un fort vernis de jargon technologique qui obscurcit leur nature profonde, la réponse à leur donner ne pourra s'abstraire de philosophie et de volonté politique. C'est vers cela que doit nous mener aujourd'hui la réflexion : quelle vision philosophique de l'équilibre entre sécurité et liberté sur les réseaux avons nous et quelle volonté politique voulons nous imprimer afin d'y aboutir ? ■

La « Balkanisation du Web », un enjeu géostratégique majeur

par Maxime Pinard,
Adjoint aux formations de l'IRIS,
Directeur de Cyberstrategia

L'affaire Snowden, qui a provoqué une immense tempête médiatique ces trois derniers mois, a eu une conséquence peu évoquée par les médias : elle a considérablement affaibli le discours officiel des autorités américaines concernant la nature du cyberespace. En effet, dans de nombreux documents officiels du Département d'Etat entre autres, les Etats-Unis mettent en garde contre toutes les politiques numériques permettant à un Etat d'accroître son contrôle du Web, prônant l'absence de frontières numériques, en d'autres termes une « homogénéisation du cyberespace » qui correspond en vérité à une « américanisation » de ce dernier, tant aux niveaux technologiques que politiques. Des critiques sont ainsi régulièrement adressées à la Chine ou à l'Iran qui chercheraient à se couper de la tutelle américaine en construisant leurs propres infrastructures, en proposant leurs propres outils numériques à une dimension réduite à la nation.

Or, les révélations sur le vaste système d'écoutes américain ont montré au grand public que le cyberespace était utilisé à des fins géostratégiques certaines par les Etats-Unis et que les puissances numériques avaient tout intérêt à s'interroger quant à leur positionnement vis-à-vis de ces derniers, pour ne pas voir leur souveraineté fragilisée. D'où un débat en Europe qui s'amorce, timidement il est vrai, quant aux stratégies à adopter pour éviter une telle dépendance vis-à-vis des Américains et surtout limiter les intrusions de ces derniers dans des secteurs économico-stratégiques majeurs. Il est vrai que les Etats-Unis demeurent pour l'instant la superpuissance numérique, renforçant leur position de leader aussi bien au niveau physique via des infrastructures numériques puissantes, qu'au niveau des logiciels et des contenus avec des entreprises majeures comme Google, Facebook ou encore Microsoft présentes dans quasiment tous les pays.

La fin de l'Internet universel ?

En abusant de leurs capacités technologiques, les Etats-Unis ont presque légitimé la nécessité pour les autres puissances d'assurer leur indépendance numérique, prenant le risque de favoriser ce qu'on a coutume d'appeler « la balkanisation du Web ». De quoi s'agit-il ? Depuis la fin des années 1990, un courant de pensée sur le Web, se référant aux guerres dans les Balkans et à leurs conséquences (éclatement de la région en plusieurs entités), cherche à mettre en garde contre une fragmentation de l'Internet tel que nous le connaissons, censé pourtant selon le dogme américain être universel et quasiment uniforme. A première vue, la menace ne semble pas crédible, et ce pour trois raisons :

1. Internet tire sa puissance du nombre de ses utilisateurs qui peuvent y accéder quasiment du monde entier. Se couper d'Internet revient à se couper du reste du monde, aussi bien en terme de contacts humains qu'en terme économique, la mondialisation des échanges s'appuyant massivement sur les capacités robustes d'Internet.

2. D'un point de vue technologique, les Etats-Unis sont pour ainsi dire le chef d'orchestre d'Internet, grâce à leur contrôle des racines du Web, leurs relais au sein des instances en charge du bon fonctionnement d'Internet (ICANN ■■■

■■■ entre autres), leur avancée certaine au niveau des outils numériques, que ce soit des logiciels (systèmes d'exploitation de chez Microsoft ou Apple) ou des services en ligne (réseaux sociaux, messagerie, achats en ligne…).

3. Une telle fragmentation pourrait aboutir à une révolution dans le cyberespace, où les Etats reviendraient au premier plan dans la définition des enjeux diplomatiques entre puissances numériques, secteur aujourd'hui fortement dirigé par les géants économiques. Cela signifierait la fin de l'Internet (utopiste ?) des années 1970 qui entendait mettre en place un nouveau modèle de gouvernance, capable de résister aux pressions politiques et économiques.

Pas un... mais plusieurs Internet !

Or, la balkanisation du Web, loin d'être un fantasme, est une réalité du cyberespace qu'il convient de prendre en compte pour ne pas manquer le tournant géostratégique qu'elle risque de constituer. En effet, depuis le milieu des années 2000, plusieurs pays ont mené des politiques visant à assurer l'intégrité de « leur » portion du cyberespace, comprenant que ce dernier n'a rien de neutre ou d'apolitique et que sa maîtrise devient indispensable avec la place toujours plus prépondérante des outils numériques dans nos sociétés. Cette balkanisation est visible dans les trois couches du cyberespace : physique, logique, sémantique. La maîtrise d'une seule couche ne saurait suffire pour assurer à un Etat son autonomie cybernétique. Par exemple, un pays aura beau inciter ses citoyens à utiliser des services nationaux, s'il n'a pas la maîtrise des infrastructures (data center, etc…), son contrôle du cyberespace sera au mieux parcellaire, au pire inefficace. Deux pays permettent de voir comment la balkanisation du Web se manifeste à des degrés divers : la Chine et l'Iran.

A. La Chine : ce pays est souvent présenté comme une puissance numérique liberticide, où la censure est érigée en dogme grâce à la fameuse « muraille numérique », censée « protéger » les internautes chinois des influences extérieures. Même si l'on ne peut nier que des politiques de contrôle de contenu existent afin de contenir les mouvements protestataires chinois qui agissent sur la Toile, il convient en même temps de préciser que les autorités chinoises ont une vision du cyberespace bien plus globalisante. Leur but est de contrôler toute la « chaîne de fabrication d'Internet » : cela passe par une autonomie en matière de gestion de noms de domaine ce qui est aujourd'hui le cas grâce à la mise en place en Chine de serveurs racines liés aux serveurs racines mondiaux mais libres dans leur gestion. Il est assez ironique de rappeler que cette connaissance des infrastructures numériques, en particulier le fonctionnement des routeurs, s'est faite grâce aux Etats-Unis et surtout grâce à la société Cisco qui a fourni du matériel à la Chine ainsi que les modes d'emploi pour contrôler ses réseaux. Au niveau des logiciels, la Chine est un des « champions » de la contrefaçon et du piratage, le taux de licences légales des systèmes d'exploitation Windows étant parmi les plus faibles du monde. Ces versions modifiées sont un manque à gagner pour la société américaine Microsoft mais constituent toujours une vulnérabilité pour les internautes chinois dans la mesure où les logiciels de Microsoft sont conçus en étroite collaboration avec la NSA. Ceci explique pourquoi les autorités chinoises, et en particulier les services de renseignement, utilisent de plus en plus le système d'exploitation (plus précisément le noyau) Linux, qui a l'avantage d'être paramétrable et modifiable à un très haut niveau. Ces systèmes ultra-personnalisés rendent par ailleurs la tâche aux hackers étrangers bien plus compliquée car ils ne connaissent que partiellement le théâtre d'opérations sur lequel ils vont s'engager.

La Chine a également réussi par un processus de « sinisation » à proposer aux internautes chinois quasiment les mêmes outils dont disposent les internautes américains : Google, Amazon, Facebook, Twitter ont ainsi leurs pendants chinois, modifiés au niveau linguistique, mais aussi au niveau des possibilités offertes (échange de photos par exemple). Même si la Chine doit rester ouverte au cyberespace mondial, elle semble avoir réussi ■■■

■■■ à se constituer un « cocon numérique », la protégeant dans une certaine mesure d'influences étrangères. La stratégie est payante pour deux raisons : la Chine est moins dépendante des politiques numériques américaines et surtout, elle s'assure une croissance économique sur le long terme certaine avec le développement d'outils spécifiques.

B. L'Iran : le cas de ce pays montre quant à lui que le choix de se créer un Internet national, que l'on pourrait d'ailleurs appeler Intranet, répond à des considérations politiques certes, mais aussi à des impératifs économiques et technologiques. Depuis plusieurs années, en particulier sous l'ère de Mahmoud Ahmadinejad, des informations des autorités iraniennes ont circulé dans la presse comme quoi le régime avait pour ambition de créer son propre Internet afin de ne plus être sous la tutelle américaine. Il est vrai que lors des élections de 2009, le régime avait pris conscience de l'importance des réseaux sociaux, où l'on pouvait suivre quasiment en direct les manifestations dénonçant les fraudes orchestrées par le pouvoir. Sans réelle stratégie numérique, les autorités ont à plusieurs reprises « coupé » Internet, profitant du contrôle direct qu'elles ont sur les opérateurs téléphoniques. Mais il ne peut s'agir que d'une solution de l'instant, d'autant plus que des technologies à bas coût permettent de créer facilement des connexions pour faire passer des messages.

Téhéran a donc décidé d'investir dans des outils numériques nationaux, en particulier pour tout ce qui concerne la messagerie électronique (courriels, réseaux sociaux) avec un double objectif : contrôler des contenus éventuellement gênant pour le pouvoir et surtout espionner rapidement et facilement les communications entre internautes iraniens. Il n'y a pas de chiffres fiables, voire même aucune donnée statistique, pour estimer le budget d'un tel projet et surtout son succès en terme d'inscrits et d'utilisateurs. Les rares informations disponibles évoquent surtout les difficultés pour l'instant insurmontables à créer un Internet national, aussi bien pour des questions budgétaires que technologiques, l'Iran n'étant pas en mesure aujourd'hui de proposer des outils aux fonctions aussi efficaces que ceux des Etats-Unis. La frilosité des autorités iraniennes, visible par les cyberattaques qu'elles mènent contre les utilisateurs iraniens de services américains (usurpation d'identités, détournement des sites de réseaux sociaux), laisse à penser que l'Internet national rêvé par certains n'est clairement pas pour demain.

La balkanisation du Web, bien que pouvant conduire à des dérives, n'est pas nécessairement une mauvaise évolution. Le cyberespace est de plus en plus le théâtre de rapports de force avec des déséquilibres majeurs, dont tirent parti les Etats-Unis avec leur avancée technologique. L'affaire Snowden a montré les abus possibles d'une telle prééminence. Créer un contrepoids à l'hégémonie américaine pourrait être une stratégie pour l'UE qui doit dans un premier temps acter de la réalité de la balkanisation du Web pour mieux s'en servir et devenir une puissance numérique majeure.

Les Etats de l'Union européenne ont aujourd'hui des compétences certaines pour remodeler le paysage cybernétique, mais l'absence de politiques communes, à même de créer des géants numériques capables de rivaliser avec les Google et Facebook, les cantonne pour l'instant à un rôle d'observateurs qui critiquent certes, mais sans se donner les moyens de leurs ambitions. Il y a pourtant urgence : le cyberespace, et Internet en particulier, n'est plus malheureusement ce lieu de partage, d'échanges d'informations. La marchandisation du cyberespace, sa politisation par les Etats mais aussi par les entreprises, oblige à une redéfinition de la place de chacun sur Internet. Il ne s'agit pas d'en appeler à un retour en force des Etats dans le processus décisionnel du cyberespace, car il peut comporter de fortes dérives (censure, affrontements, perte de liberté), mais bien de renforcer un équilibre, aujourd'hui très fragilisé par les stratégies diverses des puissances numériques. La balkanisation n'a été souhaitée que par une minorité, mais elle est aujourd'hui une tendance qui croît, et qui ne doit plus seulement être subie mais bien appropriée. ■

TOR et les enjeux de l'anonymisation

par Daniel Ventre,
Titulaire de la Chaire Cybersécurité & Cyberdéfense au CNRS (CESDIP-GERN)

L'application Onion Routing déployée en 1996 aux Etats-Unis et qui bénéficia de financements de la DARPA, est présentée comme l'ancêtre de TOR. Mais c'est après 2002 que TOR apparaît, avec un premier déploiement du réseau et une distribution du code sous licence open source MIT. Le développement de TOR s'est essentiellement poursuivi au sein des Moria Research Labs, dans le cadre de contrats avec le Center for High Assurance Computer Systems (CHACS), centre dépendant de l'US Naval Research Laboratory, spécialisé notamment dans la cybersécurité. Le projet bénéficiera au fil des ans de plusieurs sources de co-financement, dont celles de l'EFF (Electronic Frontier Foundation), de la NSF (National Science Foundation), ou encore de Google. Si les militaires sont à l'origine du projet, c'est en raison de leur intérêt pour des applications assurant la sûreté de leurs communications et l'anonymisation de leurs consultations de sites (les militaires dans leurs opérations de renseignement peuvent ainsi visiter des sites sans révéler leur identité). L'enjeu initial du développement du projet est stratégique, militaire. Il ne cherchait pas en priorité à aider les dissidents, les internautes de pays aux régimes autoritaires, ni à faire œuvre de défense des droits des individus. Des interrogations pèsent toutefois sur le niveau de sécurité offert aux utilisateurs.

Ambassades, ministères et entreprises un peu partout dans le monde, semblent avoir fait les frais de faiblesses de sécurité inhérentes au réseau, lorsqu'en 2007, le pirate suédois Dan Erstad a intercepté puis divulgué des centaines d'adresses e-mails et de mots de passe, action qui fut même qualifiée de « piratage de l'année » par le Sydney Morning Herald. Fin 2007, Julien Assange aurait démarré les activités de WikiLeaks sur la base de quantités importantes de documents interceptés sur TOR. On a évoqué les interceptions de communications qui seraient réalisées par des hackers chinois. L'application demeure quoi qu'il en soit vulnérable à de multiples formes d'attaques.

Son utilité, ses utilisations et ses utilisateurs

En raison de l'avantage essentiel qu'elle procure (anonymat), l'application peut avoir des usages multiples et des utilisateurs aux profils divers et intentions plus ou moins louables. L'application offre l'anonymat à ses utilisateurs ; elle permet d'accéder de manière anonyme – adresse IP non visible – à l'Internet ; TOR Mail est un TOR Hidden Service qui permet de recevoir et envoyer des mails de façon anonyme ; les services masqués (Hidden Services) permettent de créer des sites, d'héberger des plates-formes (créant une nébuleuse de sites identifiables par l'extension .onion.to).

1. Les défenseurs des libertés fondamentales. Avec TOR, les Etats-Unis offrent une application au service non seulement de la sécurité, mais aussi de la défense des libertés et des valeurs démocratiques, qui permet aux internautes de rester anonymes sur les réseaux : les notions de partage, de communauté, de mise à disposition de ressources, de gratuité, d'anonymat peuvent être mises au service des valeurs démocratiques. Selon l'EFF, TOR est un outil au service de la défense des libertés individuelles en ligne. TOR peut être utile aux militants, cyberactivistes, défenseurs des libertés

fondamentales (liberté d'expression, de communication), dissidents, plus généralement aux citoyens souhaitant échapper aux restrictions et au contrôle étatique. Son utilisation, au même titre que celle des réseaux sociaux, peut être enseignée aux cyberactivistes par des organisations de défense des droits de l'homme (comme par exemple la branche européenne du Robert Kennedy Centre for Justice and Human Rights, basée à Florence, qui forme les activistes à l'utilisation d'applications qui leur permettront de promouvoir la démocratie).

2. Les médias : les journalistes utilisent parfois TOR pour communiquer avec des dissidents, ou des acteurs dont la liberté de parole est contrainte dans les pays totalitaires.

3. La cybercriminalité : la délinquance sait user de l'anonymat offert, restant ainsi sous les radars des forces de l'ordre. Les détracteurs du projet qualifient à cet égard TOR de « réseau d'impunité ». Un service de formation à la cybercriminalité incluait dans ses cours une introduction à l'usage de TOR (à côté des VPN et autres techniques d'anonymat). La criminalité prend diverses formes : piratage, contrefaçon, diffusion de contenus illicites. Les délinquants profitent de l'anonymat offert par TOR pour créer des plates-formes où tout se vend : armes, drogue, identités (voir le site Silk Road par exemple), pédopornographie, hacking as-a-service , etc.

4. L'Etat : les gouvernements ont des raisons, à leurs yeux légitimes, de vouloir limiter, interdire ou contrôler l'usage de l'application :

- Assurer la sécurité intérieure, la paix sociale, prévenir le désordre, affaiblir la dissidence : en 2009 la Chine bloque l'accès au réseau TOR , mesure qui s'inscrit dans une politique plus large de limitation, contrôle ou censure des réseaux sociaux, sites internet. Ces mesures interviennent habituellement à l'approche de dates anniversaires « sensibles » (révoltes de Tiananmen, fête nationale en octobre, etc.).

- Lutter contre la cybercriminalité ou encore contre le terrorisme, c'est-à-dire toutes formes d'activités délictueuses et criminelles pouvant tirer parti de l'anonymat ou de la discrétion assurée par l'application. Dans cette perspective l'agence nationale de police japonaise (National Police Agency – NPA) envisageait en avril 2013 de demander aux opérateurs de bloquer TOR. Les autorités américaines sont parvenues à couper le fonctionnement du service d'hébergement Freedom Hosting, et son propriétaire Eric Eoin Marques a été arrêté en Irlande début août 2013. Le FSB (Federal Security Service) a annoncé en août 2013 son intention de bloquer TOR sur tout le territoire russe dans le cadre de la lutte contre la criminalité.

Les acteurs étatiques peuvent être eux-mêmes utilisateurs de TOR : l'armée américaine pour protéger ses communications au Moyen-Orient ; des ambassades, des autorités judiciaires (pour recueillir des informations, surfer de manière anonyme sur des sites à la recherche de données sans laisser traces de leur passage) y auraient eu recours. De manière plus anecdotique, il semblerait même que les administrations de certains Etats utilisent TOR afin de consulter des sites rendus inaccessibles du fait de leur propre censure !

5. Les citoyens : les mesures d'interdiction, légitimes aux yeux de certains Etats, le sont moins aux yeux des citoyens qui voient là des mesures liberticides, et l'expression d'une impuissance de l'autorité publique, incapable en effet de s'attaquer aux auteurs des exactions. La lutte contre la criminalité pénaliserait ainsi les citoyens, limiterait leurs libertés, mais ne contraindrait guère les criminels.

Les défis de l'anonymisation

Dès sa création, l'Internet a défié l'efficacité des mécanismes traditionnels de contrôle et les outils et méthodes d'anonymisation sur les réseaux contribuent à ce défi (les autres étant contenus dans le caractère transnational de l'internet et sa décentralisation). Des moyens d'anonymisation furent

■■■ même déjà mis à disposition des utilisateurs de Usenet pour poster des messages dans les newsgroups sans divulguer leur identité.

L'anonymat des communications est sujet à controverses depuis les années 1990. En effet, si son usage répond à des objectifs légitimes (il permet par exemple l'accès à l'information, l'expression libre, le contournement de la censure, le whistleblowing, de se protéger contre des régimes politiques répressifs, de fournir des informations à la police), il rend aussi possibles des actes socialement condamnables. Face à cette dualité, les Etats agissent avec plus ou moins de fermeté. Les Etats démocratiques eux-mêmes éprouvent des difficultés à gérer la liberté fournie à des utilisateurs qui deviennent insaisissables (le principe de l'anonymat étant de les rendre non localisables et non identifiables). D'autres questions se posent également : le droit à la vie privée (personal privacy) n'est-il pas parfois incompatible avec le contrôle social ? L'anonymat n'est-il pas facteur de déresponsabilisation des individus ? L'anonymat ne décrédibilise-t-il pas ?

L'anonymat sur Internet soulève des questions d'ordre technique (quelles applications sont en mesure d'assurer quel niveau de sécurité à l'utilisateur?), éthique, social, juridique (l'anonymat et la libre expression sont-ils ou non des droits fondamentaux, quelles pratiques sont légales ou non, quel rôle jouent les fournisseurs d'accès à internet et les opérateurs dans la préservation de l'anonymat, quel est le statut juridique des services de messagerie anonyme et services de re-routage de mails ?), économique (si les services d'anonymisation comme TOR sont fournis gratuitement, des entreprises proposent des formations à leur utilisation, qui elles sont payantes ; toute l'activité underground qui se développe, notamment criminelle, représente une économie dont les volumes d'activités demeurent toujours difficilement appréciables à leur juste niveau), sont autant de dimensions analysées depuis les années 1990, par exemple lors des conférences de l'AAAS (American Association for the Advancement of Science) . Mais bien que les enjeux soient donc identifiés depuis plus de 20 ans, la réelle pratique de l'anonymisation sur Internet demeure mal connue : quels sont les facteurs qui motivent le choix de l'anonymat ; quelles sont les stratégies d'anonymisation mises en œuvre ; quel est le profil des acteurs choisissant l'anonymat ; quelles leçons tirer sur un plan stratégique et technique… ?

Des études sur la question de l'anonymat, il résulte que la pratique est moralement neutre , que le principe n'est intrinsèquement ni bon ni mauvais. Il est des situations où ses effets doivent être contrecarrés pour des raisons de sécurité, mais d'autres où il doit être encouragé, toléré. Le défi pour les Etats est ainsi de parvenir à préserver ce juste équilibre entre liberté de leurs citoyens (la Cour Suprême américaine a rappelé que l'anonymat et la liberté d'expression sont des droits essentiels protégés par le 1er Amendement de la Constitution, car vitaux pour un discours démocratique) et contraintes de sécurité (l'après 11 septembre 2001 est marqué par un ensemble de mesures limitant l'anonymat, en permettant notamment aux autorités d'accéder aux données d'identification dont disposent les opérateurs et divers fournisseurs dans le cadre d'enquêtes) . Or, les restrictions touchant directement les outils, au motif de la lutte contre les agissements criminels, peuvent aussi porter un coup à l'exercice de l'anonymat par le plus grand nombre : la fermeture de l'hébergeur Freedom Hosting début août 2013 a certes mis un frein à la diffusion de contenus pédopornographiques, mais aussi coupé dans le même temps des services tels que TorMail ou Hidden Wikki ; lorsque la police japonaise envisage de bloquer l'utilisation de TOR pour lutter contre la cybercriminalité, elle le fait aussi aux dépens des utilisateurs qui eux n'ont rien à se reprocher. ■

Bitcoin : monnaie du futur, concept éphèmère ou argent des voyous ?

Entretien avec Philippe Blanc,
Directeur technique informatique et hacktiviste
Propos recueillis par Pierre-Yves Castagnac

IRIS : Bitcoin agite la planète web depuis quelques mois, mais cette monnaie virtuelle ne fait pas concensus. Les réactions sont nombreuses... et très partagées.

Philippe Blanc : Effectivement, Bitcoin, ou plutôt, le protocole Bitcoin, ne laisse pas indifférent. Pour en comprendre l'essence, revenons à la définition. Alors... de quoi s'agit-il ? Il s'agit, d'un côté, de l'unité d'une monnaie virtuelle décentralisée que l'on trouve sur Internet, et de l'autre, de la technologie qui permet à cette monnaie d'exister. Ce concept se veut expérimental, mais il commence à faire ses preuves. Des sites Internet comme eBay s'y intéressent de près, tout comme certains Etats. L'Allemagne vient par exemple de reconnaître au Bitcoin le statut de « monnaie privée ». C'est assez exceptionnel pour le souligner. Sur le plan technique, cette monnaie est générée grâce à un logiciel libre appelé « Bitcoin miner » que l'on pourrait comparer au travail des chercheurs d'or : il faut casser des cailloux (blocs électroniques) pour trouver des pépites (Bitcoins)… Et plus le temps passe, plus les blocs sont imposants rendant ainsi plus long le temps nécessaire à l'extraction de Bitcoins. On assiste à l'heure actuelle à une véritable ruée vers l'« or » car le nombre de Bitcoins disponibles dans la « mine » n'est pas infini. Onze millions de Bitcoins ont déjà été extrait sur les vingt-et-un prévus par le protocole.

IRIS : En quoi le protocole Bitcoin représente une petite révolution ?

Philippe Blanc : Cette révolution tient à la combinaison de trois points : indépendance, sécurité et anonymat. Indépendance car Bitcoin est basé sur un réseau de type peer-to-peer sans aucune autorité centrale. Une transaction Bitcoin se fait directement entre deux individus. Avec Bitcoin disparaît ainsi la notion d'« intermédiaire de confiance » : il est désormais possible d'acheter et de vendre sans qu'une personne, un organisme ou un Etat ait son mot à dire. Sécurité ensuite, car la technologie Bitcoin offre des garanties telles qu'ils en font un moyen de paiement sûr et fiable. Enfin, anonymat car le vendeur et l'acheteur peuvent se cacher derrière l'équivalent d'un pseudonyme qui peut-être changé pour chaque transaction.

IRIS : Comment est né Bitcoin ?

Philippe Blanc : L'idée de monnaie virtuelle est aussi ancienne qu'Internet mais toutes les tentatives précédentes ont échoué. L'expérience la plus réussie reste cependant le « Linden », une monnaie mise en circulation dans le jeu de réalité virtuelle Second Life. Il était possible d'acheter des Linden avec de l'argent réel (dollars, euros...) mais impossible de le dépenser en dehors du jeu… rendant in fine cette monnaie peu attirante. Bitcoin, à la différence du Linden, ne dépend pas d'un jeu ou d'une structure hermétique. Bitcoin est utilisable si les deux parties, acheteur et vendeur, possèdent le logiciel. Sur le plan historique, Bitcoin s'inscrit dans la continuité du concept de B-Money imaginé par Wei Dai en 1999. Bitcoin né officiellement dix ans plus tard, en février 2009, à la suite de la publication quelques mois plus tôt d'un document signé « Satoshi Naka moto ». – Il s'agirait d'un Japonais de

■■■ 37 ans selon sa fiche web, mais en réalité, impossible de savoir s'il s'agit de sa véritable identité. Attirés par ce concept, des passionnés de cryptographie se sont mis à tester ce protocole. Le cercle des utilisateurs s'est rapidement élargi surfant sur un effet de mode. A ses débuts, Bitcoin n'était qu'une monnaie de troc : X Bitcoin(s) contre Y objet(s) ou Z nourriture… mais il va rapidement trouver une équivalence avec le dollar US. De virtuelle, cette monnaie est ainsi devenu bien réelle. Un Bitcoin vaut aujourd'hui un peu moins de 140 dollars. J'attire votre attention sur le fait que le cours du Bitcoin a fortement fluctué dans les mois précédent, en raison, notamment, d'une forte spéculation.

IRIS : Quels sont les avantages et les inconvénients du Bitcoin ?

Philippe Blanc : Ils sont de plusieurs ordres ! Premièrement, il n'existe pas d'autorité régulatrice, le Bitcoin s'échange d'individu à individu sans passer par un intermédiaire (banque, Etat). S'il n'y a plus d'intermédiaire, il n'existe donc plus de frais sous-jacents (frais bancaire, frais de dossier…). De même, il devient impossible de geler un compte pour empêcher une transaction car l'utilisateur détient chez lui, sur son propre disque dur, son porte-monnaie Bitcoin. Deuxièmement, Bitcoin est extrêmement sécurisé ce qui rend cette monnaie virtuelle très sûre. Enfin, troisièmement, les transactions Bitcoins sont anonymes. Cependant si cette combinaison « sécurité-anonymat-indépendance » est inédite, elle est en réalité à double tranchant. En effet, sans « banque » ou « coffre de banque », cette monnaie est stockée directement sur le disque dur du porteur. Si le disque dur grille, est perdu ou est volé, tout est perdu ! Quand aux tiers de confiance qui proposent de stocker vos Bitcoins sur un serveur sécurisé, certains se sont fait pirater, d'autres sont partis avec la caisse.

IRIS : Ne pas connaître l'acheteur, ne pas pouvoir identifier le vendeur… Un rêve pour certains milieux. Je pense en particulier aux trafiquants d'armes ou encore au dealer de drogue.

Philippe Blanc : Effectivement, ce triptyque « sécurité-anonymat-indépendance » pourrait intéresser certains milieux mafieux. Vous évoquez les ventes d'arme, la vente de drogue… mais à cette liste, pourrait se rajouter toutes transactions des économies parallèles : la vente d'une voiture sous le manteau, la contrebande de vêtement, la contrebande d'objet d'art… Cependant, si Bitcoin représente bien une petite révolution technologique, Bitcoin n'est en revanche qu'un moyen « de plus », devrais-je dire, pour ces milieux. Rappelons qu'il existe déjà à leur disposition, d'autres moyens. Je pense en particulier au cash – il n'y a rien de plus anonyme – ou encore aux bons au porteur pour des transactions plus importantes. Quant à savoir si Bitcoin représente la monnaie du futur ou l'argent des traffiquants, seul l'avenir nous le dira ! ■

L'Observatoire Géostratégique de l'Information

Sous la direction de François-Bernard Huyghe, cet observatoire a pour but d'analyser l'impact de l'information mondialisée sur les relations internationales. Comprendre le développement des médias et de l'importance stratégique de la maîtrise de l'information. Il analyse, par exemple les rapports de force entre puissances politiques et économiques et les firmes qui contrôlent le flux des informations dans le Monde.

IRIS - Institut de Relations Internationales et Stratégiques
2 bis, rue Mercoeur
75011 Paris - France
contact@iris-france.org

www.iris-france.org
www.affaires-strategiques.info

Secrétariat de rédaction : Pierre-Yves Castagnac