bouclier d'or de la Chine

Les entreprises et le développement de la technologie de surveillance en Chine

entrer

par
Greg Walton

Droits et Démocratie est un organisme canadien investi d'un mandat international qui, en collaboration avec des organismes de la société civile et des gouvernements au Canada et à l'étranger, fait la promotion des droits humains et du développement démocratique par le dialogue, la sensibilisation, le renforcement des capacités et l'éducation du public. Droits et Démocratie articule son action sur quatre thématiques : le développement démocratique, les droits des femmes, les droits des peuples autochtones et la mondialisation et les droits humains ; ainsi que sur deux initiatives spéciales : la promotion des droits humains au plan international et les interventions d'urgence et occasions importantes.

L'auteur :
Greg Walton est un chercheur indépendant qui étudie surtout la question de l'impact des technologies et de la mondialisation sur les droits humains et la démocratie. Il travaille actuellement à mettre au point des « stratégies de conformité perturbatrices » pour des organismes sans but lucratif transnationaux. Sa page Web : go.openflows.org/jamyang.

Remerciements :
Carole Samdup, Diana Bronson et toute l'équipe de Droits et Démocratie. OxBlood Ruffin, cDc, Drunken Master et le projet Hacktivismo! y Oda, la cache Google, l'infrastructure Kundrel, SafeWeb, Patrick Ball, Jenny8, Wyrds of Simple Nomad, Openflows, M&D, et tant d'autres – de chaque côté du coupe-feu – qui bien sûr ont choisi de garder l'anonymat. Pour le moment.;-)

Dépôt légal : Bibliothèque nationale du Québec, quatrième trimestre 2001.
Bibliothèque nationale du Canada, quatrième trimestre 2001. ISBN : 2-922084-43-4.

Graphisme : Laperrière Communication
Imprimé au Canada

Le Bouclier d'or de la Chine 1.0 est publié sur le site www.ichrdd.ca et à titre de rapport libre sur les droits humains à : go.openflows.org.

LIBERTÉ_D'EXPRESSION : LIBERTÉ_DE_CODE

Le Bouclier d'or de la Chine

Toute personne a droit à ce que règne, sur le plan social et sur le plan international, un ordre tel que les droits et libertés énoncés dans la présente Déclaration puissent y trouver plein effet.

Article 28 de la Déclaration universelle des droits de l'homme

Selon Bill Gates, il est un peu étrange d'associer le libre-échange à des questions de droits humains : cela équivaut à s'ingérer dans les affaires internes.[1]

Bill Gates, alors chef de la direction de Microsoft,
aux côtés de Jiang Zemin au cours d'une séance de photos à Beijing, en 1994

Table des matières

Préface

On a souvent qualifié les nouvelles technologies de l'information et des communications d'élément moteur de la mondialisation. Elles ont aussi été promues comme étant un outil de démocratisation alors que la connectivité était proclamée comme marquant la fin des disparités technologiques. Il ne fait aucun doute que les communications électroniques ont facilité la circulation de l'information sur la planète ainsi que la construction d'un réseau de soutien international aux activistes luttant pour les droits humains et la démocratie.

Malheureusement, l'avènement des technologies modernes de communication a aussi lancé de nouveaux défis aux défenseurs des droits humains, surtout à ceux qui vivent dans des régimes répressifs. Dans un monde où les règles de commerce international n'ont aucun lien avec le droit international relatif aux droits humains, les priorités économiques menacent la promesse de démocratisation par les technologies. En Chine, où il n'existe ni responsabilité démocratique ni lois pour la protection des droits humains, les technologies peuvent devenir, et sont devenues, des instruments de répression.

Il y va du droit de tous les hommes à un ordre international dans le cadre duquel les promesses de la Déclaration universelle des droits de l'homme pourraient être tenues. La Déclaration, ainsi que le Pacte international relatif aux droits civils et politiques qui l'accompagne, vise à protéger les droits fondamentaux de la personne, y compris le droit à la vie privée. La protection des droits humains constitue une obligation des gouvernements et doit s'appliquer à toutes les activités de ces gouvernements, qu'il s'agisse de la promotion d'échanges commerciaux, de la négociation d'ententes commerciales bilatérales ou internationales, de financement à l'exportation ou d'aide au développement.

Le présent document montre à quel point les technologies de pointe, développées au Canada et mises de l'avant au moyen d'une série de processus nationaux et internationaux, peuvent miner les principes des ententes sur les droits humains. Le projet Bouclier d'or de la Chine menace la protection des droits de la personne, surtout le droit à la vie privée – un droit qui étaye d'autres éléments essentiels de la lutte pour les droits humains, comme la liberté d'association et la liberté d'expression. Le Bouclier d'or positionne l'alliance entre le gouvernement et les entreprises à l'opposé du cyberfront du mouvement de lutte pour le respect des droits humains en Chine.

Le présent document cherche à donner un aperçu du monde de la haute technologie, des grandes entreprises et de la lutte pour les droits humains et la démocratie en Chine. Au nom de Droits et Démocratie, je propose ce document dans un esprit de solidarité avec le peuple chinois, qui trouvera peut-être utile son contenu dans son développement et sa consolidation des mouvements sociaux pour le changement. Je l'offre également à tous mes compatriotes au Canada qui, à la lumière des récents rapports sur la surveillance policière des dissidents au Canada, pourront découvrir combien les droits des citoyens de la Chine sont étroitement liés aux nôtres.

Le président,
Warren Allmand, c.p., o.c., c.r.

Résumé

La Chine vit un paradoxe très moderne. D'une part, les dirigeants sont conscients que les technologies de l'information sont le moteur de l'économie mondiale et que la croissance économique de la Chine repose en grande partie sur l'intégration du pays à l'infrastructure mondiale de l'information. D'autre part, la Chine est un pays à régime autoritaire et à parti unique qui assure sa stabilité sociale par la suppression des activités antigouvernementales. En bref, le contrôle politique repose sur la croissance économique; celle-ci nécessite la modernisation des technologies de l'information, qui, à leur tour, peuvent affaiblir le contrôle politique.

La « grande muraille électronique de Chine » se fissure. Le gouvernement sait qu'il ne peut espérer purger l'information de tout matériel jugé « répréhensible » avant son entrée sur les réseaux de Chine. Tiraillée par ces forces contradictoires d'ouverture et de contrôle, la Chine cherche un équilibre entre les besoins en information de la modernisation économique et les exigences en sécurité pour une stabilité interne. Dans la recherche de cet équilibre, la Chine a trouvé des alliés de taille parmi les entreprises de télécommunications privées principalement en Occident. Nombreuses sont celles qui jouent un rôle déterminant dans la satisfaction des besoins en sécurité du gouvernement chinois, notamment Nortel Networks, jusqu'à tout récemment la plus grande entreprise au Canada. Nortel Networks et d'autres entreprises internationales aident en fait la Chine à remplacer sa grande muraille électronique érigée au niveau des passerelles internationales par un système plus évolué de filtrage du contenu au niveau de l'individu.

Les anciennes méthodes de censure sont en voie d'être supplantées par une architecture de surveillance massive et omniprésente : le Bouclier d'or. Le véritable objectif est d'intégrer une gigantesque base de données en ligne à un réseau de surveillance globale incorporant la reconnaissance de la parole et des visages, la télévision en circuit fermé, des cartes intelligentes, des dossiers de crédit et des technologies de surveillance d'Internet. Le FBI (Federal Bureau of Investigation) des États-Unis y prête main-forte par son ambitieux projet de normalisation de l'équipement de télécommunications pour faciliter la surveillance électronique, projet maintenant adopté comme norme internationale.

Nombreux sont ceux qui en Chine sont mis en état d'arrestation pour des « crimes » Internet, que ce soit pour avoir fourni des adresses de courrier électronique à des publications Internet ou pour avoir fait circuler de l'information en faveur du mouvement démocratique ou des articles dénonçant le gouvernement chinois, en contradiction flagrante avec le droit international relatif aux droits humains garantissant la liberté d'expression. Les dissidents sont en général accusés de « subversion » ou d'avoir « menacé de renverser le gouvernement », la distinction entre une activité criminelle et l'exercice du droit d'expression étant inexistante en Chine. Le développement de cette nouvelle architecture globale de surveillance électronique compliquera encore plus la vie de ces activistes courageux.

Le salon Security China 2000, tenu à Beijing, a attiré environ 300 entreprises de plus de 16 pays. Parmi les organisateurs : la « Commission sur la gestion de la sécurité publique du Comité central du Parti communiste chinois ». Au salon, le nouveau projet Bouclier d'or du ministère de la Sécurité publique a rapidement ravi la vedette. Son but : promouvoir l'adoption des technologies de l'information et des communications de pointe pour renforcer le contrôle policier central, améliorer les capacités de réaction, aider à mieux combattre le crime et rendre plus efficace le travail des policiers. L'appareil de sécurité de la Chine a de grandes ambitions : construire un réseau de surveillance numérique à l'échelle de la nation, permettant de relier les agences de sécurité locales, régionales et nationales dans un circuit de surveillance globale. Beijing voit le projet Bouclier d'or comme un système de télésurveillance fonctionnant à partir de bases de données avec accès immédiat aux dossiers d'enregistrement de chaque citoyen et des liens vers de vastes réseaux de caméras visant à améliorer l'efficacité des services de police.

Pour réaliser le Bouclier d'or, le gouvernement chinois s'appuie sur l'expertise technologique et les investissements des entreprises occidentales. Nortel Networks du Canada joue un rôle déterminant dans ce scénario comme le démontrent :

> ses projets de recherche en participation avec l'Université de Tsinghua pour l'adaptation de la technologie de reconnaissance de la parole à des fins de surveillance automatique des appels téléphoniques ;

> son appui d'emblée et précipité aux plans du FBI de mise au point d'une norme commune pour l'interception des communications téléphoniques, la CALEA, de concert avec le transfert technologique assuré par la coentreprise Guangdong Nortel (GDNT) ;

> son étroite collaboration avec Datang Telecom, une entreprise chinoise ayant des intérêts importants dans le marché de la sécurité publique en Chine ;

> la promotion du JungleMUX, qui permet le transfert des données vidéo d'un réseau de télésurveillance vers un centre de contrôle du ministère de la Sécurité publique (MSP) de Chine ;

> le déploiement de ses produits Internet Personnel à Shanghai, grâce auxquels les fournisseurs de services Internet peuvent beaucoup mieux surveiller les communications des utilisateurs ;

> un projet de 10 millions de dollars US pour construire un réseau optique large bande urbain (OPTera) à Shanghai permettant aux autorités de surveiller les activités des abonnés à l'extrémité du réseau, principalement au moyen du coupe-feu Shasta 5000, ce qui constitue une violation du droit à la vie privée. Il est donc de plus en plus difficile pour les

dissidents d'avoir des communications clandestines et de plus en plus facile pour la police de découvrir qui sont les utilisateurs d'Internet qui tentent d'accéder à des URL jugées non appropriées par le gouvernement chinois ;

> l'intégration des technologies de reconnaissance de la parole et des visages en collaboration avec AcSys Biometrics, une filiale de NEXUS à Burlington en Ontario.

Beaucoup d'autres entreprises occidentales ont participé au renforcement d'un appareil de sécurité répressif au moyen des développements suivants :

> une base de données nationale comprenant des données sur tous les citoyens adultes de la Chine ;

> des cartes intelligentes pour tous les citoyens, qui peuvent être lues à distance à l'insu du porteur ;

> un système de télévision en circuit fermé pour la surveillance des endroits publics ;

> la technologie qui permet au Bureau de la Sécurité publique des comparaisons instantanées d'empreintes digitales ;

> le développement de coupe-feu en Chine.

Le discours technologique actuel, préoccupé avant tout par la satisfaction de ses propres besoins, promet que les nouvelles technologies de l'information et des télécommunications seront démocratiques en soi et qu'elles favoriseront l'ouverture partout où elles seront employées. *Le Bouclier d'or de la Chine. Les entreprises et le développement de la technologie de surveillance en Chine* détruit ce mythe. La technologie fait partie intégrante d'un contexte social et, comme le montre le présent document, elle favorise la répression dans un régime à parti unique au nom de l'expansion des marchés et de profits exponentiels.

Introduction

Des télécommunications inadéquates ont depuis longtemps été le lot de la Chine. La croissance économique a exigé la modernisation d'une infrastructure caractérisée par une technologie désuète et un accès limité aux ressources nécessaires pour la développer. Pour pallier ces manques, le gouvernement s'est lancé dans un effort, bien financé, de modernisation de son infrastructure d'information. La Chine est donc devenue un des plus grands consommateurs d'équipement de télécommunications au monde.

Un objectif important de cette modernisation a été l'acquisition d'équipement de télécommunications évolué auprès des pays industrialisés, la révolution sur le plan des technologies de l'information étant perçue comme l'occasion pour la Chine de faire un pas de géant et de grandement améliorer ses capacités dans les secteurs liés aux télécommunications. Le transfert de ces technologies à la Chine a été facilité par deux tendances étroitement liées.

D'abord, les entreprises de télécommunications se livrent une concurrence féroce dans le partage du marché des télécommunications chinois, relativement peu développé mais à croissance rapide, mais surtout le plus grand marché au monde. De toute évidence, cette source potentielle de milliards de dollars attire les plus importantes entreprises de télécommunications, notamment Lucent et Cisco aux États-Unis, Nokia et Ericsson en Europe et Nortel Networks au Canada, sans compter toutes les autres. La Chine achète annuellement de ces entreprises plus de 20 milliards de dollars d'équipement de télécommunications.

La Chine représente environ 25 % du marché mondial de l'équipement de télécommunications, en pleine expansion exponentielle. Une grande partie de cette croissance est attribuable aux ventes d'équipement des entreprises de télécommunications étrangères et aux coparticipations avec des entreprises en Chine, ce qui nous amène à la deuxième tendance.

L'installation d'une infrastructure de télécommunications évoluée en vue de faciliter la réforme économique complique beaucoup les objectifs de sécurité interne du pays. Plus la quantité d'information circulant sur les réseaux de Chine augmente, plus il est difficile pour le gouvernement de contrôler cette information.

La croissance exponentielle d'Internet en Chine laisse croire à certains que les nouvelles technologies adoptées vont créer une société plus ouverte et plus démocratique. On se base sur l'hypothèse qu'Internet est en soi un moyen de démocratisation qui favorise le pluralisme, renforce la société civile et, de ce fait, force les gouvernements à rendre des comptes. Dans un monde d'après-guerre froide, le pouvoir des technologies de l'information et des communications de transformer les sociétés répressives est souvent considéré comme une évidence.

Pourtant, à la lumière des événements récents ayant eu lieu en Chine, le potentiel d'Internet comme moyen de démocratisation revêt un caractère improbable. La documentation à ce jour est éloquente : les dirigeants de la Chine ont résolument choisi de censurer le contenu en ligne et de restreindre l'accès des citoyens à l'information publiée à l'extérieur du pays.[3] Ils visent également à empêcher l'émergence de l'« organisation virtuelle » qui est devenue une importante fonction d'Internet dans les démocraties occidentales. Vu sous cet angle, Internet lance un certain nombre de nouveaux défis au régime. Selon un sondage récent mené par l'Académie chinoise des sciences sociales, 10 % des utilisateurs admettent utiliser régulièrement des

serveurs mandataires pour contourner la censure, la plupart des utilisateurs ont presque autant confiance dans les sources étrangères de nouvelles que dans les sources gouvernementales et la majorité croient qu'Internet aura un impact important sur la vie sociale et politique.[4]

Aux prises avec cette rapide transformation, les autorités chinoises sont impatientes d'acquérir les nouvelles technologies qui leur permettront d'augmenter la surveillance. Internet peut certes donner du pouvoir aux citoyens, mais il fournit également au gouvernement une nouvelle série d'outils de répression pour surveiller les échanges privés et censurer l'opinion publique.

En mars 2000, à Beijing, le président chinois Jiang Zemin (à gauche) serre la main de Frank Carlucci, président de Nortel Networks du Canada.

Dès le premier raccordement de la Chine au réseau Internet mondial en 1994, les autorités ont cherché à contrôler les liaisons Internet. Une restriction sévère de la connectivité internationale constituait le cœur de la stratégie de sécurité Internet naissante de la Chine. Aujourd'hui, sept ans plus tard, les connexions internationales des cinq réseaux principaux de la Chine sont desservies par des serveurs mandataires raccordés à des « passerelles »[5] internationales officielles. Le filtrage et la surveillance du trafic réseau s'effectuent toujours à ce niveau. Nommée par dérision la « grande muraille électronique »[6] par les pirates informatiques et les journalistes à l'échelle de la planète, cette stratégie a remporté un succès mitigé. En effet, la modernisation économique continuelle a entraîné une croissance exponentielle de la demande pour une largeur de bande internationale, et le volume actuel du trafic Internet pose un sérieux défi à la stratégie de censure par l'État au niveau des passerelles.

De nombreuses raisons expliquent la construction du réseau chinois sur ce modèle de « grande muraille électronique ». Les passerelles moduleraient le rythme de l'ouverture de la Chine au monde au moyen d'une interaction électronique. Le gouvernement pourrait décider à quel rythme augmenter les connexions et, en théorie, couper celles-ci en cas d'urgence sociale.

Les passerelles devaient constituer la première ligne de défense contre les intrusions antigouvernementales dans le réseau, une sorte de dispositif coupe-feu dont la fonction était de restreindre la quantité d'information sur les réseaux internes accessible aux intrus étrangers. Elles ont été conçues pour empêcher les citoyens de la Chine d'utiliser Internet pour accéder à des sites interdits et à de l'information antigouvernementale provenant de l'étranger. Les autorités espéraient, grâce à ce contrôle par l'État des tables d'acheminement au niveau des passerelles, empêcher les Chinois d'accéder à des sites étrangers comme ceux du Cable News Network (CNN), de la British Broadcasting Corporation (BBC), du Réseau d'information du Tibet (Tibet Information Network) ou de Human Rights Watch/Asia.

Les règlements et les lois de la Chine régissant Internet reposent sur le principe d'« ouverture prudente » dans le but de préserver les avantages économiques de l'accès à des réseaux d'information mondiaux tout en protégeant le pays contre la domination économique étrangère et l'utilisation d'Internet par des groupes internes ou étrangers à des fins subversives. Les enjeux sont élevés, pour le gouvernement alors que la Chine se joint à l'économie mondiale et pour le « cyberdissident » potentiel, qui risque la peine de mort pour avoir utilisé Internet illégalement.

Encadré 1 :

Le prix de la liberté

En janvier 2001, l'agence de presse officielle Xinhua annonçait que toute personne impliquée dans des « activités d'espionnage » comme « le vol, la pénétration, l'achat ou la divulgation de secrets d'État » au moyen d'Internet ou par tout autre moyen risquait la peine de mort ou une peine d'emprisonnement allant de dix ans à la réclusion à vie.

> Le 18 janvier 2000, Leng Wanbao était interrogé pendant trois heures après avoir fait circuler une lettre d'un autre dissident à l'extérieur de la Chine sur Internet.La police a rappelé à Leng Wanbao que l'envoi d'une telle lettre contrevenait aux lois sur la sécurité publique.

En 1998, Lin Hai, un entrepreneur en logiciels, est accusé de subversion pour avoir fourni des adresses de courrier électronique chinoises à un magazine Internet prodémocratique.

> Le 3 mars 2000, les autorités chinoises relâchaient Lin Hai, un entrepreneur en logiciels, qui avait été condamné à deux années de prison pour avoir incité des personnes « à renverser l'État ».Arrêté en 1998, Lin Hai était accusé d'avoir fourni 30000adresses de courriel chinoises à des publications dissidentes outre-mer, notamment *VIP Reference*. Les adresses ont servi à distribuer des articles dissidents sur Internet.Relâché dans le plus grand secret en septembre 1999, Lin Hai hésitait beaucoup à parler de sa situation, suggérant que les autorités l'avaient libéré plus tôt que prévu en échange de son silence. À sa sortie de prison, Lin Hai s'est qualifié de « premier prisonnier Internet chinois ».

> Le 3 juin 2000, Huang Qi, directeur du site www.6-4tianwang.com comprenant un forum de discussion, a été arrêté et accusé de « subversion», plus précisément d'avoir publié sur son site Web hébergé aux États-Unis des articles qui condamnaient le massacre de Tienanmen en juin 1989.Le site publiait une lettre de la mère d'un jeune étudiant tué durant le massacre ; celle-ci encourageait la reprise du mouvement prodémocratique de 1989.L'ordinateur de Huang Qi ainsi que tous les documents trouvés à son bureau et à sa résidence furent confisqués. Le site, ouvert à « tous ceux qui ont quelque chose à dire », est toujours maintenu par des Chinois dissidents vivant aux États-Unis, mais les utilisateurs d'Internet en Chine ne peuvent plus y accéder.

> Le 16 août 2000, la police interrogeait Jiang Shihua, un professeur en informatique de la province de Sichuan, dans le sud-ouest de la Chine. On l'accusait d'« incitation à la subversion ».Il avait utilisé son cybercafé, le Silicon Valley Internet Coffee, à Nanchong, pour faire circuler des articles qui critiquaient les autorités et pour publier des articles prodémocratiques dans un groupe de discussion Internet. Il a été accusé d'« incitation à renverser l'État ». Il n'a pas encore comparu devant les tribunaux.

> Le 19 septembre 2000, Qi Yanchen, rédacteur en chef de la publication en ligne *Consultations,* était reconnu coupable de « subversion» et «d'avoir fait circuler de l'information antigouvernementale sur Internet» et condamné à quatre ans de prison.Le Bureau de la Sécurité publique (BSP) prétend qu'il a utilisé le pseudonyme Ji Li pour écrire des articles pour le mensuel *Kaifang* de Hong Kong et le bulletin dissident *VIP Reference.* Il aurait aussi publié des extraits de son livre *The Fall of China,* qui appelle à une réforme politique. La police a confisqué son ordinateur, son télécopieur et ses notes.

> Le 13 mai 2000, le gouvernement suspendait les activités du site China Finance Information Network pour deux semaines et condamnait ses propriétaires à une amende. La publication financière en ligne était accusée d'avoir fait courir « des rumeurs qui pouvaient ternir l'image du gouvernement » après la publication d'un article sur la corruption d'un responsable politique régional.

> Le 3 août 2000, les responsables de la sécurité débranchaient et interdisaient le site www.xinwenming.net pour avoir fait circuler de « l'information contre-révolutionnaire » et attiré « une grande partie de la communauté dissidente de Chine ». Les cinq dissidents responsables du site sont actuellement recherchés par la police mais n'ont pas encore été arrêtés. Créé le 29 avril 2000, www.xinwenming.net est le premier site hébergé en Chine qui invitait ouvertement à la « réconciliation nationale et àladémocratie».

Transfert des technologies et convergence des politiques

Le droit à la liberté d'opinion, d'expression et d'information
Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit.

Article 19 de la Déclaration universelle des droits de l'homme

La mondialisation affaiblit le contrôle national de la circulation des données. Le développement d'Internet est peut-être le meilleur exemple d'une technologie mondiale. La combinaison mondialisation et convergence numérique a dans plusieurs pays en développement un effet dévastateur sur la vie privée. Dans le domaine des technologies de l'information et des communications, la vitesse de la convergence des politiques augmente tellement rapidement que même les pays les plus développés doivent forcer l'allure pour rattraper les progrès de la technologie. Dans la sphère de la surveillance numérique – écoute en ligne, systèmes d'identification personnelle, exploration de données, censure ou chiffrement –, ce sont invariablement les pays industrialisés qui établissent les règles du jeu pour le reste du monde.

Fait de plus en plus inquiétant, cette technologie de surveillance est exportée, sans se préoccuper des fins de l'acquéreur, vers des pays qui violent de manière flagrante les droits humains fondamentaux de leurs citoyens. Les gouvernements des pays dont les infrastructures sont sous-développées comptent sur les pays industrialisés pour leur fournir de l'équipement de surveillance. Le transfert des technologies de surveillance d'un pays développé à un pays en voie de développement est devenu un composant important de l'industrie de l'armement de l'après-guerre froide.[8] La normalisation transfrontalière, avec le peu d'attention qu'elle prête aux variations dans le respect des droits humains, porte plusieurs à croire qu'une architecture mondiale de surveillance électronique est en train de naître et que celle-ci émane des responsables de l'application des lois aux États-Unis.

Opération Root Canal

Dès 1988, dans le cadre d'un programme surnommé « Operation Root Canal »[9] au sein du Federal Bureau of Investigation (FBI) des États-Unis, les fonctionnaires chargés de l'application des lois dans ce pays demandaient aux compagnies de téléphone de modifier leur équipement pour faciliter l'interception des appels. Toutes les grandes entreprises internationales de télécommunications, à l'exception d'une seule, ont refusé de se plier à cette demande. L'exception était Nortel Networks, une entreprise canadienne, qui a accepté de travailler en collaboration étroite avec le FBI.[10] Plus de 75 % du trafic principal Internet nord-américain passe par les systèmes de Nortel et un important pourcentage des revenus de cette dernière provient du marché des télécommunications des États-Unis.

Après plusieurs années de lobbying par le FBI, le Congrès des États-Unis a adopté en 1994 la Communications Assistance for Law Enforcement Act (CALEA).[11] La CALEA oblige les transporteurs terrestres et cellulaires ainsi que les fabricants d'équipement de télécommunications à s'assurer que tout leur équipement, toutes leurs installations et tous leurs services permettent au gouvernement d'intercepter toute communication, filaire ou non, transmise par le télécommunicateur au moment de sa transmission.[13] Les communications doivent s'effectuer de manière à pouvoir être transmises à une installation distante du gouvernement.[14]

L'adoption de la CALEA fut controversée, le FBI cherchant continuellement à amender le projet de loi pour y inclure des règlements de plus en plus astreignants, comme ceux en vertu desquels les téléphones cellulaires doivent permettre le repérage de l'emplacement sur demande et les compagnies de téléphone doivent fournir l'équipement nécessaire pour jusqu'à 50 000 écoutes en ligne simultanées.[15]

Le FBI faisait pression non seulement sur le Congrès et sur les compagnies aux États-Unis pour l'adoption de la CALEA, mais aussi sur les alliés des États-Unis pour que la loi devienne une norme internationale. Le FBI a d'abord sollicité les ministres de la Justice et de l'Intérieur des pays de l'Union européenne (UE) pour la création de normes techniques internationales sur l'écoute électronique.[16] En 1991, le FBI a tenu une série de réunions secrètes avec les pays membres de l'UE pour les persuader d'intégrer la CALEA aux lois européennes. En 1993, le FBI organisa, à son laboratoire de recherche de Quantico en Virginie, des séminaires consacrés au développement de standards internationaux en matière d'interception des télécommunications, baptisés International Law Enforcement Telecommunications Seminars (ILETS). Des représentants du Canada, de Hong Kong, de l'Australie et de l'Union européenne y participèrent. Résultat : l'adoption d'une norme technique internationale de surveillance, la « International Requirements for Interception ».[17]

Selon un rapport de l'UE,[18] la stratégie prévoyait que les pays industrialisés s'entendent sur des normes et des procédures puis qu'ils vendent leurs produits aux pays en voie de développement. Même si les pays industrialisés refusaient de se plier aux ordres d'interception, les communications sont quand même surveillées par le réseau Signals Intelligence UK-USA « dès qu'ils utilisent l'équipement ».[19] Les efforts du FBI furent récompensés : en janvier 1995, le Conseil des ministres de l'UE adoptait discrètement une résolution dont le texte est presque mot pour mot celui des exigences nationales du FBI.[20] La résolution ne fit l'objet d'aucun débat officiel et n'a été rendue publique qu'à la fin de 1996.

Les ILETS se poursuivirent. Des comités furent mis sur pied pour élaborer une norme plus détaillée dans le but d'étendre la portée des standards d'interception. La nouvelle norme devait s'appliquer à un grand éventail de technologies des communications, notamment Internet et les communications par satellite, et établir des exigences plus détaillées relatives à la surveillance de toutes les technologies. Résultat : un document de 42 pages, ENFOPOL 98 (la désignation de l'Union européenne pour les documents produits par le Groupe de travail sur la coopération policière de l'Union).[21]

En 1998, le document est rendu public et soulève beaucoup de critiques. Les comités réagissent en produisant un nouveau document, ENFOPOL 19, expurgé de la plupart des détails controversés, mais qui en revanche étend le type de surveillance pour y inclure les adresses IP, les numéros de cartes de crédit et les adresses de courrier électronique.[22] En avril 1999, le Conseil propose la nouvelle ébauche d'une résolution en faveur de l'adoption des normes ENFOPOL 19 dans les lois de l'Union européenne.

En mai 1999, le Parlement européen approuve la résolution ENFOPOL 19. Le vote a lieu un vendredi soir en présence de 20 % seulement des délégués et est ensuite renversé par le Conseil des ministres. Ce rejet n'a pas empêché l'Institut européen pour les normes de télécommunications (ETSI) de poursuivre son travail d'élaboration de normes internationales sur l'écoute en ligne.

Que voulez-vous que soit Internet ?

« Un contact humain. Je veux qu'il sache qui je suis. »[23]

Au salon tenu à Beijing en novembre 2000, les plus grands noms en technologie Web – des entreprises qui s'associent fièrement outre-mer à la réputation anarchiste d'Internet[24] – tentaient de vendre leur marchandise à la police secrète et aux fonctionnaires de la sécurité de la Chine. Qualifié de « plus grande exposition de sécurité nationale », le salon Security China 2000 était le deuxième événement de ce genre commandité par le ministère de la Sécurité publique (MPS) en autant d'années. Parmi les organisateurs, la « Chinese Communist Party Central Committee's Commission for the Comprehensive Management of Social Security »[25] (Commission sur la gestion de la sécurité publique du Comité central du Parti communiste de Chine) est responsable de l'appareil de sécurité de l'État dans son ensemble, du contrôle des travailleurs itinérants et des campagnes anticrimes jusqu'à la surveillance des activités des dissidents.

Le *Shanghai Business Magazine* a récemment évalué à 15 % la croissance annuelle de l'industrie chinoise de la sécurité. Outre-mer, les spécialistes ont prédit dans le journal *Security World* une croissance de 20 % au cours des trois à cinq prochaines années. On s'attend à ce que, dans les dix prochaines années, la Chine devienne le deuxième marché de sécurité au monde, précédé des États-Unis.[26]

Le salon, organisé par la société Adsale Exhibition Services Ltd. de Hong Kong, a attiré environ 300 entreprises de plus de 16 pays de même que 24 500 visiteurs de plus de 26 provinces de Chine. Parmi les invités spéciaux : Jia Chunwang, ministre de la Sécurité publique. Selon Adsale, le salon Security China 2000, comparativement à celui de 1998, affichait une augmentation de 50 % du nombre d'exposants internationaux et de 80 % de la surface d'exposition.[27] Les géants de l'industrie des réseaux s'y côtoyaient : Siemens, Motorola, Cisco Systems, Sun Microsystems et Nortel Networks, entourés d'entreprises des États-Unis, d'Israël, de France, d'Allemagne, des Pays-Bas, du Japon et du Canada, parmi d'autres. Le Royaume-Uni, chef de file mondial en télévision en circuit fermé, occupait une section spéciale.

Le projet Bouclier d'or

Au salon Security China 2000, le nouveau projet Bouclier d'or du ministère de la Sécurité publique a rapidement ravi la vedette. Son but : promouvoir l'adoption de technologies de l'information et des communications évoluées pour renforcer le contrôle policier central, améliorer les capacités de réaction, aider à mieux combattre le crime et rendre plus efficace le travail des policiers.[28] L'appareil de sécurité de la Chine a de grandes ambitions : construire un réseau de surveillance numérique à l'échelle de la nation, permettant de relier les agences de sécurité locales, régionales et nationales dans un circuit de surveillance globale. Beijing voit le projet Bouclier d'or comme un système de télésurveillance fonctionnant à partir de bases de données avec accès immédiat aux dossiers d'enregistrement de chaque citoyen et des liens vers de vastes réseaux de caméras visant à améliorer le temps de réponse de la police lors de manifestations.

Même si le projet n'en est qu'à ses débuts, les chefs de l'industrie chinoise présents au salon ont évalué que le gouvernement avait dépensé 600 millions RMB (70 millions de dollars US) en recherche et que le total des dépenses s'élèverait à maintes fois ce montant.

Le projet Bouclier d'or, selon l'information disponible sur le site Web du salon, porte principalement sur les secteurs suivants de la sécurité : contrôle de l'accès, systèmes anti-piratage informatique, sécurité des communications, logiciels et accessoires informatiques, chiffrement et déchiffrement, sécurité du commerce électronique, sécurité d'Internet et des intranets, dispositifs coupe-feu, communications réseau, sécurité et gestion de réseau, sécurité des transactions, sécurité des cartes intelligentes, sécurité des systèmes, détection de virus, services TI et autres.[29]

La réussite du projet Bouclier d'or repose sur un grand éventail de technologies évoluées. Bien que la recherche technologique en Chine ait fait des pas de géant dans ces secteurs et dans d'autres domaines, les scientifiques chinois n'ont développé aucun des composants nécessaires à la réalisation du projet Bouclier d'or de manière autonome. Ils ont toujours été appuyés par les entreprises occidentales, qui leur vendent des solutions clés en main ou qui leur transfèrent la technologie au moyen d'ententes commerciales officielles ou souvent en contrepartie d'un accès plus grand au marché.

Les technologies nécessaires pour supporter un réseau intelligent de surveillance de masse sont d'une complexité affolante. Toutefois, puisque les solutions ont pour modèle les formes humaines d'intelligence, on peut, pour en parler, utiliser des termes qui nous sont familiers. Le réseau de surveillance Bouclier d'or de Beijing doit « voir », « entendre » et « penser ».

La technologie qui permet au réseau d'« entendre » – par exemple de surveiller automatiquement les conversations téléphoniques, à la recherche de mots et de phrases clés – repose sur le traitement des signaux de conversation. Pour sa part, le traitement des signaux vidéo permet au réseau, par le biais de caméras de surveillance, de « voir » – par exemple de reconnaître des visages dans une foule. Ces deux « sens », deux types de traitement numérique des signaux (DSP), sont appelés « systèmes algorithmiques de surveillance » parce qu'ils analysent les données au moyen d'algorithmes complexes modelés sur le système nerveux humain. Dans le traitement des signaux de conversation par exemple, la cochlée pourrait servir de base pour l'abstraction mathématique.

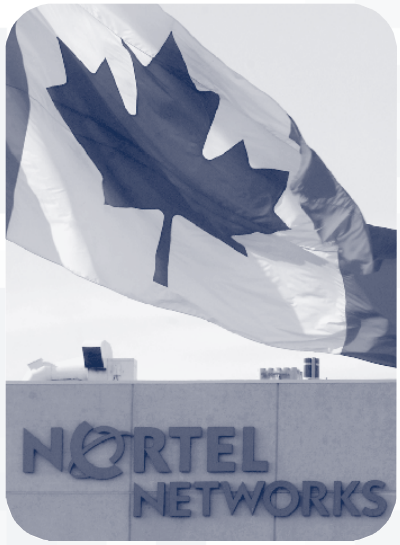
En Chine, le chef de file dans ce domaine est le Département d'ingénierie électronique de la prestigieuse Université de Tsinghua. Une équipe de recherche de ce département travaille sur la reconnaissance de la parole depuis le début des années 80. Cette recherche est financée par le gouvernement de Chine et par Nortel Networks (de 1995 à 1998)[30] et menée en parallèle avec celle de Nortel sur la reconnaissance de la parole, en collaboration avec le FBI.

Les fonds du gouvernement de Chine alloués au projet de reconnaissance de la parole proviennent des budgets nationaux alloués aux projets 863 sur la technologie de pointe.[31] Un projet 863 a débuté en mars 1986, en réaction au projet de défense stratégique « Guerre des étoiles » de l'administration Reagan.[32] Ce projet 863 accorde les investissements du gouvernement en priorité à sept volets distincts qui comportent des applications militaires et de sécurité de l'État, dont la technologie de l'information, et les systèmes à laser et antisatellites. Certains projets 863 sont supervisés par l'agence chinoise de développement de l'armement (Chinese Weapons Development Agency).[33]

À la fin de 1998, les ingénieurs de Tsinghua annonçaient qu'ils mettaient au point un grand système de reconnaissance de la parole continue à vocabulaire étendu indépendante du locuteur sur voie téléphonique. Ce système en temps réel est utilisé par les dispositifs téléphoniques et les systèmes de service d'information sur des liaisons téléphoniques, avec un taux de reconnaissance de plus de 98 %.[34] Ces ingénieurs prétendaient orienter la recherche vers la reconnaissance de la parole continue à vocabulaire étendu (voire illimité) indépendante du locuteur et la reconnaissance de la parole à vocabulaire étendu téléphonique pour mettre au point une technologie qui s'adapte rapidement à la voix du locuteur afin d'améliorer l'exactitude de la reconnaissance de la parole indépendante du locuteur.[35] Cette recherche est parallèle au développement de la technologie nécessaire à l'application de la CALEA aux États-Unis. En d'autres mots, il semble que cette recherche n'a pas d'autre but que la surveillance automatique des communications téléphoniques.

Une alliance inconvenante

Le département d'ingénierie de Tsinghua entretient des relations étroites avec le laboratoire de Recherches Bell-Northern (BNR) à Montréal, une filiale de recherche et développement de Nortel,[36] où fut mis au point le module de reconnaissance de la parole de Nortel. Au cours de sa mission commerciale en 1998, le premier ministre Jean Chrétien a annoncé que Nortel Networks et Tsinghua établiraient un laboratoire de recherche commun.[37] Un des objectifs premiers du laboratoire de recherche était d'augmenter l'expertise en réseau de la Chine. L'entente comprenait également un « programme d'échange d'experts » entre Nortel Networks et l'Université Tsinghua pour une meilleure collaboration. En effet, des diplômés du département d'ingénierie de Tsinghua ont joué des rôles déterminants dans la mise au point du module de reconnaissance de la parole de Nortel.



Encadré 2 :
Les projets « Golden » de la Chine :
« Modernisation » de l'économie de la Chine

Les projets Golden étaient des initiatives de la Chine dans les domaines des télécommunications et des infrastructures d'information dans les années 90. Ils étaient répartis en quatre phases :

La phase I regroupait quatre projets : **Golden Bridge** – l'infrastructure du réseau d'information économique national de la Chine ; **Golden Gate** (douanes) – un réseau d'information sur le commerce extérieur raccordant le ministère du Commerce extérieur et de la Coopération économique au Bureau des douanes ; **Golden Card** – un projet expérimental sur l'argent électronique ; et **Golden Sea** – un système d'information reliant les chefs du gouvernement de la Chine et leur permettant d'accéder aux données de toutes les institutions et organisations et de tous les bureaux soumis à la juridiction directe du Comité central du Parti communiste.

La phase II visait à mettre les réseaux d'information au service de la réforme économique. **Golden Macro** – le groupe financier et économique central du gouvernement pour un macro-contrôle des activités économiques nationales ; **Golden Tax** – un réseau de données reliant le centre de vérification de l'administration fiscale de l'État à Beijing à 50 bureaux régionaux et 800 centres de service ; et **Golden Intelligence** – le service Internet de la Chine.

La phase III se rapportait aux applications sectorielles du nouveau programme TI. **Golden Enterprise** – la construction d'intranets dans 12 000 grandes et moyennes entreprises de Chine et leur interconnexion en fonction des différents cercles d'affaires ; **Golden Agriculture** – un réseau de banques de données pouvant fournir de l'information sur l'agriculture, des rapports météorologiques et de l'information sur les marchés ; **Golden Health** – le système d'échange d'information du ministère de la Santé publique pour les hôpitaux ; **Golden Information** – un réseau reliant divers services de collecte de statistiques en Chine ; et **Golden Housing** – une base de données de renseignements sur le secteur immobilier à l'échelle nationale.

La phase IV comprenait le projet **Golden Cellular** – un consortium national des plus grands fabricants d'équipement de communications mobiles en Chine ; et **Golden Switch** – un programme pour la construction d'une industrie nationale de fabrication d'autocommutateurs numériques en Chine.

Tsinghua a établi des statistiques sur les formes phraséologiques courantes utilisées pendant un appel téléphonique. Deux cent quatorze formes de différentes commandes ont été dénombrées. Tsinghua a mis au point la plus grande base de données sur la parole en Chine.[38]

Étant donné l'engagement précoce de Nortel dans l'élaboration de normes appuyant la CALEA, il est bien normal que le premier autocommutateur numérique à être offert sur le marché et à offrir aux fournisseurs de services la possibilité de se conformer à la CALEA soit fabriqué par Nortel.[39]

Les commutateurs DMS Supernode sont fabriqués en Chine, le résultat d'une coentreprise avec le gouvernement chinois, la GDNT (Guangdong Nortel). Nortel affirmait à l'époque que ce transfert de technologie contribuerait énormément au développement de l'industrie des télécommunications en Chine.[40]

Nortel a investi 37 millions de dollars supplémentaires dans la GDNT (cette somme s'ajoutant au financement accordé selon le protocole d'entente de 1993 avec la commission de planification de l'État) – un investissement qui emboîtait le pas à l'annonce du gouvernement des États-Unis de compenser les fabricants d'équipement pour l'application de la CALEA.[41]

Au-delà de la grande muraille électronique : de la censure à la surveillance

Le rythme et l'ampleur du développement du réseau Internet en Chine ont réduit l'importance de la « grande muraille électronique » constituée de passerelles reliées à un intranet national sécurisé. L'idée de départ d'établir un intranet à l'échelle de la Chine a été dépassée par les événements, plus particulièrement par la libéralisation du secteur des télécommunications de la Chine.

Malgré la politique officielle d'ouverture que suggère l'entrée prochaine de la Chine dans l'Organisation mondiale du commerce, certains fonctionnaires chérissent toujours l'idée d'un réseau d'information chinois isolé des dangereuses tentations du WWW. « La Chine doit bâtir un réseau national indépendant d'Internet », a déclaré Jiang Mianheng, fils de Jiang Zemin et vice-président de l'Académie chinoise des sciences, au cours d'une conférence à Shanghai en juin dernier.[42]

Par contre, le concept des passerelles a survécu, bien qu'en partie ébranlé par des facteurs financiers et techniques. Le nombre de raccordements et le débit de transmission ont augmenté en réponse à la demande croissante des entreprises et des utilisateurs. En effet, la vitesse passait de 84,64 Mbit/s (été 1998) à plus de 351 Mbit/s (fin de 1999) et à plus de 2,5 Gbit/s (2001). Les exigences de sécurité et de contrôle ont cédé à la demande économique pour des réseaux à convergence large bande.

Les implications de la mise en place de dispositifs coupe-feu pour empêcher les Chinois d'accéder à du matériel interdit sur des sites à l'extérieur du pays sont bien connues. Bon nombre des technologies utilisées pour la sécurité informatique peuvent servir à restreindre les droits humains et la démocratie au moyen de l'intimidation et de la surveillance systématique de la population.

Le ministère de la Sécurité publique a annoncé l'an dernier que d'ici trois ans il aura créé une base de données nationale contenant les renseignements personnels et les numéros d'identification de chaque adulte au pays. Le gouvernement chinois a toujours maintenu un fichier cumulatif (appelé *dangan*) sur la performance et les attitudes de chaque personne à partir de la maternelle jusque sur le marché du travail. Cette information sera numérisée et chaque Chinois recevra une nouvelle carte d'identification de deuxième génération dotée d'une micropuce contenant son *dangan*. Actuellement, la carte d'identification est en papier laminé avec photo, et indique le nom de la personne, sa date de naissance et son numéro d'identification. Cette carte papier « est relativement facile à contrefaire », a récemment affirmé Qiu Xuexin, le directeur du plus important institut de recherche soumis à la juridiction du Bureau de la Sécurité publique,[43] à la quatrième foire internationale de la carte intelligente (Fourth International Fair of Smart Cards). Qiu a ajouté que, grâce aux techniques évoluées de chiffrement, il sera plus difficile aux personnes non autorisées à le faire d'accéder aux renseignements du gouvernement contenus dans la nouvelle carte. La seconde génération de carte intelligente sera fort probablement une « carte de proximité », c'est-à-dire qu'elle pourra être balayée instantanément à une distance de plusieurs pieds et à l'insu du porteur.[44]

En mai dernier, le ministère de la Sécurité publique (MSP) a installé chez les fournisseurs de services Internet deux boîtes noires – des dispositifs de surveillance destinés à surveiller le contenu et les activités des comptes de courrier électronique. En outre, les autorités travaillent avec des experts en technologie de l'Université Shenzhen à la mise au point d'un « système de filtrage des courriers électroniques » capable de déceler les messages « indésirables » à l'insu

du destinataire ou du moins sans son consentement.[45] Tout récemment, le MSP a participé à la création de faux serveurs mandataires pour surveiller les navigateurs qui tentent de contourner les coupe-feu officiels.[46]

Comme en 1998, Security China 2000 a été tenu en même temps que son événement frère, Building China 2000. Le projet Bouclier d'or prévoit la construction d'immeubles intelligents et certains fournisseurs font la promotion de leurs systèmes aux deux salons. Datang Telecom, une entreprise chinoise récemment impliquée dans un cas d'espionnage industriel contre Lucent, annonçait, à la suite de ces deux expositions, qu'elle avait décroché un contrat de construction d'un immeuble intelligent pour le Bureau de la Sécurité publique provincial de Jilin.

En vertu du contrat, Datang Telecom doit assurer la conception et l'implantation du projet en accomplissant toutes les tâches, notamment l'installation du système de surveillance, du câblage intégré et des réseaux informatiques. L'implantation de ce projet concrétise et rend plus visible le projet Bouclier d'or qui sera bientôt réalisé dans le secteur de la sécurité publique nationale.[47]

Sur un site Web consacré à la promotion du projet Bouclier d'or, le MSP annonçait récemment d'autres plans semblables sur l'intégration des réseaux de surveillance CCTV (télévision en circuit fermé) dans l'environnement urbain à Guangdon.[48]

Datang a également mis au point son propre logiciel de filtrage du courrier électronique et un certain nombre de coupe-feu. Elle jouit de relations privilégiées avec des fabricants outre-mer d'équipement de télécommunication, entre autres pour des projets conjoints de recherche et de transfert des technologies. Datang a bénéficié par exemple d'un projet de recherche conjoint avec Nortel portant sur le protocole sans fil CDMA, à partir duquel elle a mis au point la version chinoise du protocole : TD-SCDMA.

Bien que la Chine ait incontestablement ses propres programmes de recherche évoluée et qu'elle mette au point ses propres systèmes de sécurité, elle s'appuie essentiellement sur l'expertise fournie par des entreprises transnationales et des partenariats, sur le transfert de technologie et sur des investissements directs, et ce, même pour la technologie de base.

Bien sûr, les entreprises ne se vantent pas de telles relations. Motorola, par exemple, fournit des dispositifs de communication sans fil à la police chinoise responsable de la surveillance de la circulation routière. Or, des journalistes ont raconté qu'au salon Security China 2000, ses représentants ont refusé de répondre à leurs questions sur la participation de Motorola au projet Bouclier d'or. Orin Li, de Compaq China, est resté tout aussi évasif, en affirmant que son entreprise « n'était pas la seule », que « tout le monde le faisait » et en encourageant le journaliste à aller interroger la compagnie Sun.[49]

Sun Microsystems est certainement engagée dans le transfert de haute technologie à l'appareil de sécurité de la Chine. Elle a mis au point, en collaboration avec Hongda Group de Changchun, chef de file en technologie de reconnaissance des empreintes digitales, un réseau informatique reliant les 33 commissariats de police provinciaux, formant ainsi la couche du projet Bouclier d'or qui permet au Bureau de la Sécurité publique de comparer instantanément des empreintes digitales avec une base de données nationale.

Fournisseur d'un grand nombre de routeurs et de dispositifs coupe-feu au réseau de Chine, Cisco Systems est un autre exemple. Au salon Security China 2000, une représentante de ce géant en réseaux informatiques a affirmé au groupe de fonctionnaires du Bureau de la Sécurité publique que Cisco était le chef de file mondial en coupe-feu et que la Chine constituait un énorme marché potentiel pour ce type de technologie.[50]

Le droit à la vie privée

Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Article 12 de la Déclaration universelle des droits de l'homme

Un des défis que doit relever l'appareil de sécurité de la Chine en conséquence du déclin de l'efficacité de la « grande muraille électronique » est de passer de dispositifs coupe-feu qui filtrent le contenu à l'échelle nationale à un filtrage au niveau des habitations et des bureaux, soit la redistribution de la grande muraille électronique, de cinq passerelles internationales à des millions d'ordinateurs personnels et de cellulaires.

L'impact de cette stratégie est énorme sur la vie privée des utilisateurs puisque la surveillance des citoyens par le gouvernement devient une réalité et qu'elle fait appel à des technologies qui restreignent fortement la liberté d'expression des utilisateurs chinois d'Internet. Il devient beaucoup plus difficile pour les activistes défenseurs des droits humains et de la démocratie de communiquer à l'insu du gouvernement avec des sources d'information « illégales ».

Cette tendance, c'est-à-dire ce déplacement d'un contrôle du contenu généralisé au niveau d'une passerelle vers une surveillance des utilisateurs aux extrémités du réseau, est facilitée par les nouvelles technologies de gestion du contenu transmis sur large bande.

Au salon Security China 2000, Nortel Networks vantait au ministère de la Sécurité publique son réseau de surveillance numérique JungleMUX et sa gamme de produits OPTera Metro. JungleMUX est un système d'avant-garde de transport des images vidéo d'un réseau de télésurveillance à un centre de contrôle. Les produits OPTera Metro sont le point d'appui de l'initiative « Internet Personnel » de Nortel. Ils permettent aux fournisseurs de services Internet de mieux surveiller les utilisateurs d'Internet et leurs activités en ligne. Les défenseurs du droit à la vie privée aux États-Unis ont fortement dénoncé cette pratique.[52]

La présentation de Nortel au salon Security China 2000 a sûrement fait de l'effet. Shanghai Telecom (ST) a récemment annoncé qu'elle avait choisi les produits OPTera de Nortel pour son futur réseau optique large bande urbain de la prochaine génération. Que signifie ce contrat, évalué à plus de 10 millions de dollars US ? Que Nortel construira le premier réseau optique urbain en Chine et qu'elle fournira un système d'accès large bande et une solution ADSL qui assureront le service numérique haute vitesse à environ 200 000 abonnés. Le projet devrait être terminé à temps pour assurer les services Internet et de vidéoconférence à la réunion des chefs d'État de l'APEC prévue à Shanghai en octobre 2001. Shanghai, principale animatrice de la nouvelle économie chinoise, pourra se vanter de posséder un des réseaux urbains les plus évolués au monde.

Grâce aux produits OPTera, au cœur de la stratégie « Internet Personnel » de Nortel, Shanghai Telecom a pu construire un réseau optique parallèle évolué pouvant prendre en charge la diffusion multimédia en temps réel et autres transactions sensibles aux délais. Il est très difficile d'obtenir la diffusion multimédia en temps réel sur des circuits Internet ordinaires. Bien que les liaisons optiques d'avant-garde de Nortel permettent d'augmenter radicalement

la largeur de bande disponible à la ville de Shanghai, ce n'est pas ce qui intéresse ceux qui cherchent à protéger le réseau de Chine contre de nouvelles menaces de plus en plus sophistiquées. Les produits OPTera d'intérêt certain sont ceux sur lesquels repose la stratégie Internet Personnel : Shasta et Alteon,[53] de Nortel. Grâce à ceux-ci, Shanghai Telecom (ST) pourra offrir des services Web personnalisés aux entreprises et aux consommateurs, c'est-à-dire personnaliser les services de livraison du contenu au moyen d'un réseau conscient du contenu et de l'utilisateur. Le réseau peut « penser », soit identifier les abonnés lorsqu'ils entrent en communication, faire correspondre des noms à des adresses IP et apprendre à connaître les goûts des abonnés en matière de contenu.

Le Shasta 5000 BSN alimente l'extrémité abonné du réseau, là où les technologies « locales », comme la DSL de haute qualité, sont raccordées au réseau principal Internet et là où les abonnés accèdent aux services et au contenu large bande. Shasta est un point de regroupement universel où accès commuté, DSL, connexions filaires et sans fil, liaisons relais de trames/technologie ATM et lignes privées se raccordent à Internet. Pour ST, l'avantage concurrentiel que procure Shasta est un réseau de services large bande à valeur ajoutée. En raison du nombre de caractéristiques de sécurité qu'il recèle, Shasta constitue également un avantage pour le Bureau de la Sécurité publique de Shanghai, le plus évolué des services policiers en ligne de la Chine.

> « Imaginez un réseau qui sache qui vous êtes, où vous êtes et qui puisse vous joindre sur votre cellulaire tout comme sur votre ordinateur. Mieux, imaginez qu'au lieu de trouver votre contenu Web, ce soit vous qu'il trouve. Une affaire personnelle. Exactement. »[51]
>
> **– Nortel Networks, Stratégie Internet Personnel**

La stratégie Internet Personnel est présentée à ST comme elle l'est en Occident, c'est-à-dire comme un moyen d'augmenter les profits générés par les réseaux en offrant entre autres des services de sécurité ou en permettant la revente de données à d'autres entreprises. Cette pratique de revente de données - personnelles, condamnée par les défenseurs du droit à la vie privée, est formellement exclue dans la déclaration de confidentialité de Nortel. Pourtant, la stratégie Internet Personnel repose sur la capacité du réseau à faire correspondre des adresses IP aux profils démographiques des utilisateurs.

Nortel présente sa stratégie Internet Personnel comme la clé du futur d'Internet. C'est pourquoi cette stratégie occupe le centre de sa dernière campagne de publicité. Il est tout à fait remarquable que Nortel puisse promouvoir auprès d'autres entreprises des pratiques commerciales qu'elle affirme exclure de ses propres activités.

Grâce à Internet Personnel de Nortel, le Bureau de la Sécurité publique de Shanghai peut faire bien plus que simplement surveiller les accès au Web en ciblant certains auditoires et en créant des profils démographiques en temps réel. Un tel système de distribution et de livraison sur réseau intelligent a un impact formidable sur la vie privée des utilisateurs. Internet Personnel est un réseau qui sait toujours « qui vous êtes ».

Les utilisateurs qui accèdent au réseau au moyen de diverses technologies d'accès comme la DSL, l'accès par câble ou l'accès sans fil reçoivent des paramètres de sécurité qui sont appliqués par abonné. Doté d'une capacité extraordinaire de traitement de paquets, Shasta est l'une des plus puissantes plates-formes de classe transporteur pour la gestion de la sécurité réseau. Le service large bande de marché de masse et la connectivité permanente entraînent de nouvelles inquiétudes sur le plan de la sécurité. Le Shasta 5000 BSN offre des

fonctions étendues de coupe-feu faciles à fournir et permettant la surveillance en permanence du flux de transmission de chaque individu.

L'accès large bande contraste avec l'accès commuté classique en vertu duquel les abonnés communiquent avec leur fournisseur de services Internet (FSI), font leur petite affaire puis coupent la communication. La nature brève de l'accès commuté n'offre guère le temps d'exploiter un point faible de la sécurité. Par conséquent, les incidents de sécurité au moyen de l'accès commuté sont peu nombreux et sans grande envergure.

« Nortel Networks s'engage à ne pas vendre, louer ni divulguer ces informations auprès d'autres organisations. »[54]

« Nortel Networks collecte les adresses IP pour l'administration du système et le suivi interne. Lorsque vous visitez notre site, nos serveurs consignent seulement les adresses IP. Nous ne lions pas les adresses IP à des informations personnellement identifiables. »[55]

– Déclaration de confidentialité de Nortel,2000

Les entreprises disposant de liaisons d'accès spécialisées (T-1, relais de trames) sont protégées. Mais, en raison du coût élevé de ces liaisons, les petites et moyennes entreprises, les consommateurs, les groupes d'intérêt et les organismes non gouvernementaux hésitent à y avoir recours. Ils utilisent des accès large bande qui sont raccordés en permanence à Internet. Pourtant, actuellement, la plupart des utilisateurs de la DSL ou du câble sont raccordés à Internet sans coupe-feu et sont par conséquent très vulnérables. Cette question constitue une vraie menace pour la sécurité des réseaux.

L'extrémité abonné

Pour contrer cette menace, Shasta de Nortel offre une couche de sécurité qui se positionne entre les coupe-feu personnels et des solutions d'entreprise bien plus coûteuses. Ce produit intègre une fonction évoluée de coupe-feu basée sur des politiques et sur des états, avec authentification à distance, enregistrement des activités, chiffrement et filtrage du contenu. Shasta étant situé à l'extrémité du réseau, le fournisseur de services peut appliquer ses politiques de sécurité à chaque abonné au moyen d'une interface au lieu de laisser aux abonnés le soin de gérer la sécurité.

L'« extrémité abonné » est le point de regroupement dans le réseau du fournisseur de services, soit le point de contact entre l'abonné et le réseau. Il s'agit du seul point dans le réseau où le fournisseur de services peut « voir » l'abonné et contrôler les flux de données. Au-delà de ce point, le trafic de plusieurs abonnés est regroupé sur des connexions haute vitesse et acheminé vers des routeurs principaux. Lorsque le trafic parvient à la passerelle internationale, il est impossible pour les agences de surveillance de distinguer les flux individuels de trafic.

La solution de sécurité de Nortel repose sur le principe suivant : le seul point viable dans le réseau où le fournisseur de services peut appliquer quelque forme de contrôle que ce soit sur le trafic d'un abonné est à l'extrémité abonné. En d'autres mots, même si le logiciel de sécurité est situé dans le PC de l'abonné, il est géré à distance par son FSI. Cette stratégie marque la fin de la « grande muraille électronique », puisque la surveillance et le contrôle du contenu

s'effectuent maintenant sur le trafic à l'extrémité du réseau plutôt qu'en son centre, c'est-à-dire au niveau d'une passerelle internationale.

Une autre fonction de sécurité importante de Shasta : une technologie évoluée qui empêche la contrefaçon d'adresses IP. La contrefaçon informatique consiste à envoyer du trafic à partir d'une adresse IP apparemment autorisée et par conséquent acceptable par le coupe-feu, alors qu'il s'agit en fait d'une adresse dont s'est emparé le pirate pour une utilisation illégale. Même les coupe-feu les plus évolués peuvent être trompés par un bon pirate. Le Shasta 5000 BSN peut empêcher les pirates d'accéder au réseau d'un abonné parce qu'il applique des fonctions anticontrefaçon au niveau de chaque abonné. Le coupe-feu Shasta 5000 BSN peut filtrer le trafic en provenance ou à destination d'un abonné et empêcher l'utilisateur final de produire des paquets contrefaits ou de transférer le trafic d'un autre abonné.

Les répercussions sont multiples. Tandis que le produit améliore la protection contre les attaques de type interruption de service, il présente tout un défi aux systèmes créés pour aider ceux qui tentent de contourner les coupe-feu de la Chine, notamment les dissidents et les activistes en faveur de la démocratie.

Une ombre virtuelle

Les fournisseurs de services procèdent à la vérification de l'identité pour valider l'accès des utilisateurs à leurs réseaux. Les mécanismes d'authentification sont nombreux : nom d'utilisateur et mot de passe, cartes intelligentes, dispositifs biométriques tels que les balayeurs d'empreintes digitales et les systèmes de reconnaissance des visages.

Le Shasta 5000 BSN permet plusieurs types d'authentification des utilisateurs, en fonction du mécanisme et du protocole d'accès. Par exemple, pour l'accès d'un administrateur au Shasta 5000 BSN, l'authentification s'effectue actuellement au moyen d'un mot de passe, mais l'authentification biométrique n'est pas exclue.

L'enregistrement des activités permet d'effectuer un suivi des activités au sein du réseau et à son extrémité pour déterminer si le trafic rejeté constitue une menace ou respecte un plan ordonné. Ces renseignements peuvent ensuite servir à améliorer les fonctions de sécurité du réseau et à justifier la surveillance d'utilisateurs « illégaux ».

Le Shasta 5000 BSN fournit une interface utilisateur graphique (IUG) pour la création et la définition de l'enregistrement de toutes les activités ainsi qu'un gestionnaire de journal qui affiche chaque événement enregistré par abonné et par service. L'information du journal est stockée puis acheminée vers des bases de données distantes. Tous les événements, incluant l'acceptation ou le rejet de paquets, peuvent être enregistrés dans un journal en fonction de

critères système et sont horodatés au moment où ils se produisent. Tous les paquets abandonnés en raison de leur non-conformité à un comportement « normal » de protocole peuvent également être enregistrés dans le gestionnaire de journal à des fins d'analyse.

Le gestionnaire de journal de Shasta permet l'analyse, le filtrage et la recherche dans le journal, et ce, de différentes façons, afin d'extraire rapidement et efficacement de l'information très détaillée sur les habitudes de communications d'une personne. Cette information peut ensuite être stockée dans d'énormes bases de données locales et centralisées où elle demeure disponible pour d'autres analyses par le MSP. Celui-ci peut par exemple établir des correspondances entre de « vrais » événements et des habitudes de trafic Internet. Une montée subite inhabituelle du nombre de courriels envoyés pendant la journée avant une manifestation, par exemple, produirait beaucoup de données même sans avoir accédé au contenu des messages.

Le filtrage du contenu constitue un autre moyen de contrôler le contenu Internet entrant dans n'importe quel environnement – à la maison, à l'école, au cybercafé et au bureau. Des filtres bloquent, dans une circonstance ou un environnement particulier, certaines URL qui répondent à des critères ou font partie de certaines catégories. Des centres régionaux de sécurité Internet sous le contrôle du MSP et exclusivement réservés à la maintenance de ces listes d'URL s'établissent dans toute la Chine pour faciliter, sur le plan local, l'application de la stratégie de contrôle de l'information du gouvernement.

Le filtrage est assuré au moyen de serveurs mandataires qui vérifient chaque demande Web individuelle en la comparant avec une liste d'URL interdites et en bloquant tout contenu provenant de ces URL ou qui ne répond pas aux critères du gouvernement définissant un contenu Web « sain ». Grâce à sa capacité de réacheminement vers de tels sites de serveurs de filtrage de contenu, le Shasta 5000 BSN peut prendre en charge ces services mandataires.

En effet, grâce à la fonction d'acheminement selon des politiques du Shasta 5000 BSN, le trafic d'un abonné peut être acheminé vers des serveurs de filtrage de contenu qui effectuent ce traitement pour le gouvernement.

Ce contrôle du contenu sur le plan local entraîne deux conséquences majeures pour toute personne en Chine qui tente d'accéder au contenu d'une URL de la liste « noire » du MSP. En premier lieu, il sera beaucoup plus difficile d'accéder aux sites Web proscrits puisque les fonctions de coupe-feu du Shasta sont beaucoup plus évoluées, étant situées au point de raccordement du PC de l'utilisateur à Internet. Par exemple, l'utilisation de serveurs mandataires situés à l'extérieur de la Chine, une pratique courante chez les dissidents pour contourner les coupe-feu au niveau de la passerelle, sera décelée beaucoup plus facilement et enregistrée pour donner un profil d'utilisation qui, avec le temps, paraîtra suspect.

En deuxième lieu, grâce à une gestion du filtrage de contenu au plan régional, les bureaux du MSP seront beaucoup plus impliqués dans le processus d'optimisation des données de surveillance à partir de sources de haute technologie et de leur utilisation dans des scénarios moins pointus – intégrant des données Internet à des modes classiques de surveillance du MSP comme les réseaux d'informateurs. Ce processus est impossible à gérer centralement sauf pour les cas les plus en vue, mais devient un puissant moyen de contrôle s'il est appliqué au niveau des régions, des villes et des quartiers.

Un réseau qui sait qui vous êtes et où vous êtes

Droit à la liberté d'association
Toute personne a droit à la liberté de réunion et d'association pacifiques.

Article 20 de la Déclaration universelle des droits de l'homme

Un des objectifs du projet Bouclier d'or est d'établir un réseau national de télévision en circuit fermé ou de caméras CCTV dans des endroits publics pour réduire le temps de réponse des policiers lors de manifestations.[57] Les caméras de surveillance exposées au salon Security China 2000 montraient bien la grande complexité de la nouvelle technologie. De nouveaux types de circuits permettent à la caméra d'ignorer les objets brillants qui émettent de la lumière dans son champ ; la miniaturisation rend les caméras presque invisibles ; les caméras à infrarouge assurent la surveillance dans l'obscurité.

Selon Gerrit Hurenkamp, directeur du développement à Pelco International aux États-Unis, le marché de la télévision en circuit fermé en Chine représente annuellement de 350 à 400 millions de dollars US. Un marché lucratif mais difficile à pénétrer. Les Chinois sont très éduqués et savent ce qu'ils veulent. On ne peut pas leur vendre n'importe quel produit.

Les dispositifs électroniques de surveillance vidéo de plus en plus évolués exigent une plus grande largeur de bande pour le transport des images produites à des emplacements distants vers des centres de contrôle. L'architecture du réseau doit être assez évoluée pour desservir un pays aussi étendu que la Chine et, dans la présentation de son système JungleMUX au salon Security China 2000, Nortel abordait directement cet aspect. Les signaux vidéo sur circuit fermé sont transportés dans le réseau JungleMUX de Nortel sur un réseau longue distance (WAN) à des vitesses de 1,6 à 44 Mbit/s et sont accessibles par tous les nœuds du réseau. Chaque source vidéo (caméra, magnétoscope, etc.) est numérisée au moyen d'un algorithme de compression configurable par l'utilisateur : une solution de transport CCTV efficace et évolutive.

Les modes d'enregistrement sont divers : en temps réel, de qualités diverses, et en chrono-cinématographie. L'enregistrement en temps réel est comme celui en télévision ordinaire (30 images par seconde, animation intégrale). La chronocinématographie est un procédé de prise de vues accélérée (quelques images par période). L'avantage de ce procédé est qu'une bande magnétique peut enregistrer pendant plus longtemps qu'en temps réel, une fonction fort utile pour l'archivage : les images couleur haute résolution 700 x 480 à deux images par seconde utilisent 400 kbit/s par caméra. La souplesse d'attribution de largeur de bande du mappeur vidéo JungleMUX permet l'enregistrement d'images de meilleure résolution et d'un plus grand nombre d'images par seconde pour une caméra en particulier, en tout temps (jusqu'à une qualité de diffusion de 700 x 480, 30 images/s, signaux couleur NTSC, utilisant environ 6 Mbit/s [qualité MPEG-2]). Le système offre même des voies audio pour bruit ambiant pour les applications de surveillance publique.

La surveillance urbaine atteindra un tout nouveau plateau de contrôle, dès qu'un logiciel fiable de reconnaissance des visages deviendra la norme. Ce logiciel sera d'abord déployé dans les

Encadré 3 :

Technologie « neutre » sur la place Tienanmen

Après le massacre de la place Tienanmen en 1989, les autorités chinoises ont torturé et interrogé des milliers de personnes pour tenter d'identifier les organisateurs de la manifestation. Même si les étudiants et les travailleurs avaient résisté au régime de terreur de la police secrète, les infortunés manifestants n'avaient aucune chance de rester dans l'anonymat. La place Tienanmen est surveillée par un réseau de caméras fabriquées au Royaume-Uni, conçues pour surveiller et régulariser la circulation. Ces caméras ont enregistré toutes les activités des mois précédant l'arrivée des tanks sur la place.

Dans les jours qui suivirent, les images prises par ces caméras furent diffusées à répétition sur la chaîne de télévision nationale. Presque tous les transgresseurs furent ainsi identifiés. Siemens Plessey, fabricant et exportateur des caméras, et la Banque mondiale, qui a payé pour leur installation, prétendent qu'ils n'avaient aucune idée que leur équipement « technologiquement neutre » serait utilisé à ces fins. Toutefois, en 1995, la Banque mondiale a accordé les fonds pour établir le même système de contrôle de la circulation à Lhassa, la capitale de la Région autonome du Tibet, qui jusqu'ici ne s'est jamais plainte de problème d'embouteillage. En outre, la zone surveillée par le système de contrôle de la circulation est entièrement réservée à l'usage des piétons.[56]

emplacements comme les tourniquets, les douanes et les passages de sécurité pour assurer la reconnaissance standard du visage vu de face. C'est le début d'une révolution en surveillance algorithmique – l'application efficace de l'intelligence artificielle à l'analyse de données au moyen d'algorithmes complexes permettant la reconnaissance et le suivi automatiques. Une telle automatisation ne fait pas qu'élargir le filet de surveillance, elle en rétrécit les mailles.[58]

Au premier rang de cette révolution : AcSys Biometrics Corp., une entreprise en participation de AND Corporation, inventeur et développeur de la technologie d'intelligence artificielle Holographic/Quantum Neural Technology, HNeT, et de NEXUS, une société de gestion de Burlington en Ontario exploitant un réseau très diversifié de filiales autonomes et de partenariats.[59] AcSys Biometrics est un fournisseur d'un des systèmes de reconnaissance des visages les plus évolués sur le marché. Le Système de reconnaissance des visages d'AcSys (Face Recognition System [FRS]) fait maintenant partie de la gamme des produits de Nortel. Il est basé sur une technologie exclusive visant à établir rapidement et de manière fiable l'identité des personnes. Il s'agit d'une solution évolutive facile à intégrer aux systèmes et aux applications en place utilisant des protocoles réseau standard.

En rapport avec la stratégie Internet Personnel, Rick Collins, premier directeur, ProtoNet: Disruptive Solutions Implementation, à Nortel Networks, affirme que l'intégration des fonctions de reconnaissance des visages d'AcSys aux solutions de Nortel Networks rendra encore plus personnels les réseaux de communication. Les gens pourront être reconnus à l'emplacement. On ne devra plus, pour ce faire, utiliser des services mobiles. Il envisage un réseau qui sait qui vous êtes, éventuellement où vous êtes, et qui peut vous joindre que vous utilisiez un téléphone mobile ou un PC.[60]

Le système de reconnaissance de la parole et des visages d'AcSys Biometrics repose sur un module breveté d'intelligence artificielle appelé Holographic/Quantum Neural Technology (HNeT). Les réseaux neuronaux HNeT pourraient prendre en charge un grand nombre d'applications de Nortel dans les secteurs financier, manufacturier, médical, de la sécurité et

de la surveillance. Les technologies comme HNeT, permettant des vitesses d'apprentissage de 200 fois celle des réseaux neuronaux classiques, rendent bel et bien réelle la reconnaissance des visages sur CCTV et sont perçues par les pays dotés d'infrastructures CCTV comme une évolution naturelle de leurs réseaux. Comme le démontre l'exemple des systèmes de contrôle de la circulation installés sur la place Tienanmen et à Lhassa, l'amélioration des fonctions des systèmes de surveillance signifie une subtile érosion des droits humains. Les dynamiques de ce processus sont simples : le développement continuel de la technologie et l'utilisation de celle-ci à des fins autres que celles prévues.

Diagramme 1 :

Un nouveau modèle pour Internet : l'innovation à l'extrémité du réseau

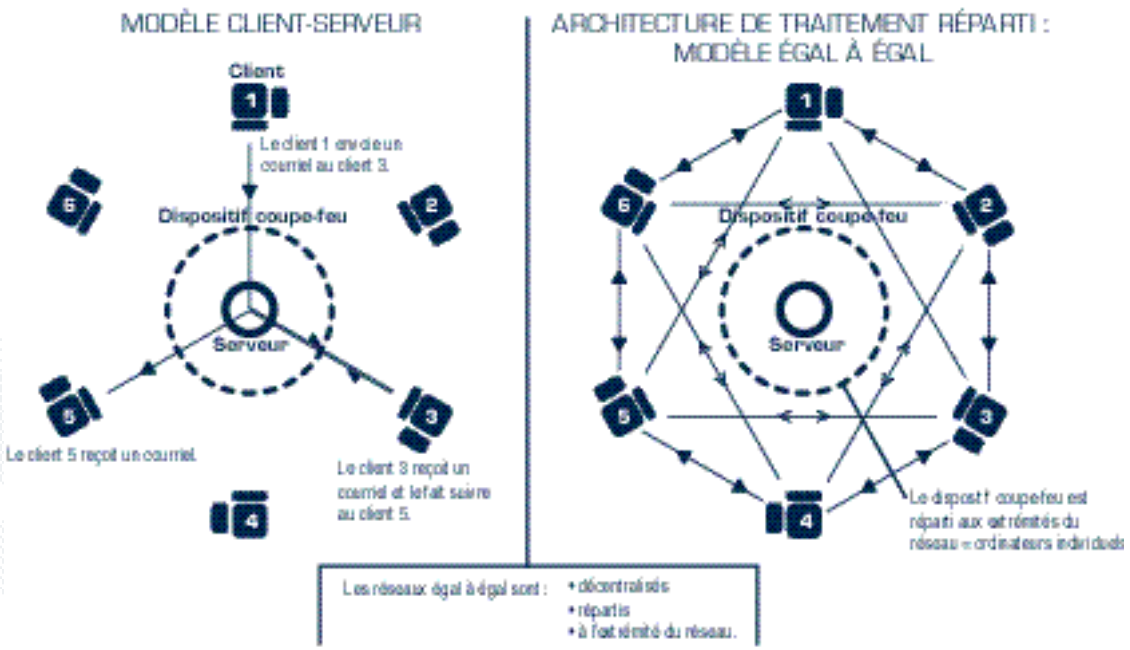
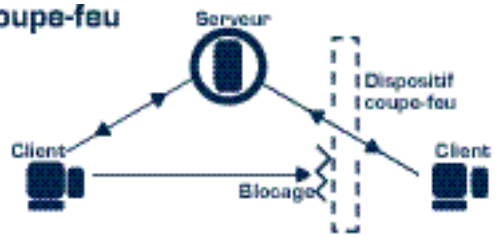


Diagramme 2 :

Interaction en présence d'un dispositif coupe-feu

Le logiciel d'égal à égal permet aux utilisateurs de communiquer directement entre eux par défaut. Quand un dispositif coupe-feu rend la communication directe impossible, la plupart des logiciels d'égal à égal dirigent automatiquement les messages vers un service de relais centralisé, pour l'acheminer sous tunnel vers l'accès 80.



Conclusion

« La souris est plus forte que le missile »

La seule chose qui distingue la stratégie Internet Personnel de Nortel, la recherche sur la reconnaissance de la parole ou la technologie CCTV des instruments de répression est la responsabilité démocratique. En Chine, les concepts de « sécurité de l'État » et de « secrets d'État », qui sont le fondement de la réglementation sur le contenu Internet et qui obligent les fournisseurs de services à surveiller les utilisateurs, ont toujours été utilisés pour restreindre la liberté d'expression, bloquer les organismes indépendants et supprimer de l'information. En Chine, le droit à la vie privée n'existe pas et aucun recours légal n'existe non plus pour tenir le gouvernement responsable de son utilisation de l'information obtenue par son appareil de sécurité au moyen de la surveillance, de l'écoute en ligne ou de la surveillance en ligne de communications électroniques.

En Chine, comme dans tous les pays du monde, les activistes qui se portent à la défense des droits humains livrent un nouveau combat : s'assurer que l'innovation technologique est au service de la liberté et de la démocratie et ne devient pas une forme subtile et évoluée de répression. Bon nombre des entreprises qui exposent leur marchandise au salon Security China 2000 prétendent partager cet objectif en soutenant qu'elles agissent pour améliorer la qualité de vie et de travail des gens (Philips) et pour que les gens puissent rester en contact, partout et en tout temps, avec les ressources dont ils ont besoin (Sun Microsystems).

Dans la pratique, toutefois, d'autres mesures ont besoin d'être mises en place pour que ces belles phrases soient plus qu'un simple exercice de relations publiques. Tandis que les prédicateurs de la mondialisation parlent de « règles du jeu équitables » et de « systèmes basés sur des règles », des millions de gens en Chine vivent dans un système de contrôle politique qui a un impact sur chaque aspect de leur vie. On ne peut parler de règles du jeu équitables sans liberté, ni de systèmes basés sur des règles lorsque ces règles ne gouvernent que la dimension commerciale de l'interaction humaine et que l'État viole constamment les droits humains fondamentaux.

Les gouvernements démocratiques, dont celui du Canada, doivent donner la priorité à la promotion des droits humains dans tous les aspects de leurs relations internationales, incluant les échanges commerciaux et les investissements. En 1995, dans son énoncé de politique étrangère *Le Canada dans le monde,* le gouvernement du Canada proclamait son engagement : «… nous utiliserons efficacement toute l'influence que nous confèrent nos relations économiques et commerciales et notre aide au développement pour promouvoir le respect des droits de la personne. »

Devant un forum d'organisations non gouvernementales tenu à Montréal en 1998, le ministre canadien des Affaires étrangères et du Commerce international, Lloyd Axworthy, avait tenu les propos suivants :

« Nous sommes ici pour discuter d'une technologie qui révolutionne le monde – qui modifie les rapports de force, remet en question les circuits de communication conventionnels,répand et dissémine au maximum l'influence – et démocratise ainsi les voies de transmission en se débarrassant de ceux qui veulent les contrôler… parce que le potentiel de cette technologie de forcer les barrières,de surmonter les obstacles d'ordre politique – d'éduquer, d'informer et d'être un agent de changement politique – est proprement ahurissant… la souris est plus forte que le missile. »[61]

Malheureusement, en Chine, la technologie ne sert pas une cause aussi noble. Les multinationales au premier rang de la révolution de l'information ne peuvent prétendre que leur seule présence en Chine garantira un meilleur respect des droits humains; les gouvernements ne peuvent s'obstiner à croire que les marchés ouverts mèneront automatiquement à la démocratie. Dans les pays à régime autoritaire et oppressif où la lutte contre le crime est volontairement confondue avec la répression de la dissidence, des règles différentes doivent être appliquées pour orienter le développement politique et social. Ignorer ce défi, c'est compromettre la liberté en Chine, certes, mais c'est aussi, dans nos sociétés en voie de mondialisation, mettre en péril la liberté de tous.

Annexe

Comment utiliser le CD-ROM qui accompagne le présent document

Installation :

Suivez les instructions ci-dessous pour installer le CD-ROM pour Windows 95/98/ME/2000 et Mac OS.

1. Fermez toutes les applications et ouvrez le lecteur de CD-ROM.
2. Déposez le CD-ROM dans le lecteur, face graphique vers le haut.
3. Une fois le lecteur fermé, une fonction d'exécution automatique lance le programme d'installation.

Si votre ordinateur n'est pas doté d'une telle fonction ou que cette fonction est désactivée, vous pouvez lancer le programme d'installation, appelé chinags.exe, comme suit :

Windows: Double-cliquez sur l'icône Poste de travail de votre bureau. Double-cliquez ensuite sur l'icône correspondant à votre lecteur de CD-ROM puis sur l'icône chinags.exe.

Mac: Cliquez sur l'icône CD-ROM du bureau puis sur l'icône chinags.exe.

Textes de la pochette

> ***Les moyens de distribution de ce rapport – surtout sa version chinoise – sont aussi importants que le contenu du rapport lui-même.***

> **En raison de la législation régissant Internet en Chine – surtout en ce qui concerne notre obligation de fournir l'accès aux lecteurs chinois – et au cours de la recherche et de la distribution de ce rapport, un certain nombre d'outils et de concepts libres ont été utilisés. Ils sont expliqués brièvement ci-dessous.**

> **Si vous voulez accéder à la version en ligne de ce rapport (à go.openflows.org) à partir de la Chine, veuillez utiliser le logiciel anticensure-antisurveillance fourni sur le CD-ROM.**

> **La version en ligne du rapport ainsi que celle fournie sur le CD-ROM comportent des renseignements supplémentaires sur le processus de recherche, y compris un aperçu des règlements et de la législation de la Chine régissant les communications électroniques.**

Cette année, à la conférence Linux World, Lawrence Lessig, professeur de droit à l'Université de Stanford, a lancé le défi de s'engager et de combattre le pouvoir des « anciens ».[62]

Lessig, célèbre pour sa contribution au droit Internet et auteur du livre *Code and Other Laws of Cyberspace,* a décrit comment une législation désuète, le monde financier, le gouvernement et les grandes entreprises ont détourné à leur profit la « plate-forme libre » que devait être Internet, idéologiquement conçue pour favoriser la libre expression, mais devenue un outil de répression de l'innovation.

M. Lessig a demandé à son auditoire : « Que voulez-vous faire à ce sujet ? Je ne pourrai pas arrêter ce changement. Plus je parle et moins on (le gouvernement et les entreprises) veut m'écouter, moins on veut entendre cette histoire. Mes efforts sont inutiles dans cette lutte. Ceux qui peuvent faire une différence, c'est vous, les gens qui ont construit cette architecture de liberté. »

Hacktivismo !

« Hacktivismo et le CULT OF THE DEAD COW publient la présente déclaration pour exprimer leur indignation et affirmer leur intention d'agir. La déclaration Hacktivismo est notre Magna Carta pour le droit à l'information. La population a droit à un accès raisonnable à toute information publiée légalement. Si nos dirigeants ne sont pas prêts à défendre Internet, nous le sommes. »

« A Special Message of Hope », 4 juillet 2001[63]

Patrick Ball

« L'Hacktivismo place la technologie au service des droits humains », selon Patrick Ball, directeur adjoint du programme Human Rights de l'American Association for the Advancement of Science, qui a participé entre autres à des projets d'enquête des Nations Unies sur les crimes de guerre et les génocides ainsi qu'à des projets sur les droits humains au Guatemala, en Haïti et en Afrique du Sud.

PGP

De nombreux groupes de défense des droits humains utilisent des logiciels de cryptographie ou de chiffrement comme PGP (Pretty Good Privacy) pour protéger leurs messages, ce qui est souvent une question de vie ou de mort. PGP empêche l'information de tomber entre les mains de personnes autres que les destinataires et vérifie si les messages sont authentiques au moyen de signatures numériques. Son impact sur le respect des droits humains est énorme. [Voir CD-ROM.]

Rubberhose

(prononcé Marutukku)

Rubberhose a d'abord été conçu par le programmeur en cryptographie Julian Assange comme outil pour les militants des droits de la personne et les journalistes qui devaient protéger des données confidentielles comme des listes d'activistes ou des détails concernant des violations de droits.

Les programmeurs de Rubberhose ont rencontré des groupes de militants des droits humains et entendu des récits de ces violations. Les militants doivent souvent transporter, dans des situations extrêmement dangereuses, des portables contenant des données essentielles. Ils sont parfois arrêtés par des patrouilles militaires qui n'hésiteraient pas à torturer un suspect pour obtenir le mot de passe leur permettant d'accéder aux données.

Freenet

Freenet est un énorme réseau P2P qui regroupe la puissance des ordinateurs membres dans le monde entier pour créer un dépôt d'archives ouvert à tous ceux qui désirent publier ou consulter des renseignements de tout type. La version 1.0 du présent rapport est publiée en trois langues sur Freenet. Elle est accessible à la Chine et au reste du monde. [Voir CD-ROM.]

SafeWeb

Internet en Chine, le catalyseur d'un changement social ?

SafeWeb est un service mandataire anonyme à chiffrement SSL actuellement utilisé environ 100 millions de fois par mois par des centaines de milliers de personnes dans le monde. Il est le site Web le plus populaire au monde.

Triangle Boy est un programme libre qui permet à des bénévoles de transformer leur PC en passerelle dans le réseau SafeWeb afin d'empêcher les gouvernements répressifs de censurer Internet. Triangle Boy a recours à des techniques de contrefaçon d'adresses IP et de transmission par paquets pour réduire la consommation de largeur de bande sur les ordinateurs des bénévoles. [Diagramme 2 : Interaction en présence d'un dispositif coupe-feu.]

Acheminement (tables d'acheminement)
Processus permettant de diriger les paquets entre les points d'origine et de destination dans un système interconnecté. L'acheminement est généralement effectué par un dispositif spécialisé appelé *routeur*. La fonction d'acheminement est une fonction importante du réseau Internet parce qu'elle permet de relayer les données d'un ordinateur à un autre, jusqu'à ce qu'elles parviennent à destination. Les ordinateurs intermédiaires accomplissent cette tâche en transmettant les données reçues au prochain ordinateur. Pour déterminer le meilleur parcours, les ordinateurs consultent des tables d'acheminement.

Adresse IP
Numéro unique composé de quatre groupes de chiffres séparés par des points. Exemple : 163.113.245.2.
Tous les ordinateurs reliés à Internet sont identifiés par une adresse IP unique. Un ordinateur qui n'est pas identifié par une adresse IP n'est pas vraiment relié à Internet. La plupart des ordinateurs sont également identifiés par un nom de domaine, plus facile à mémoriser.

ADSL (ligne numérique à paire asymétrique)
Technologie qui permet de transmettre des données sur les lignes téléphoniques classiques. Beaucoup plus rapide que le service téléphonique ordinaire, la technologie ADSL utilise la même paire de fils de cuivre que le service téléphonique ordinaire. Le circuit ADSL doit être configuré pour relier deux emplacements particuliers, comme une ligne spécialisée. L'ADSL peut atteindre des vitesses de téléchargement de 1,544 Mbit/s, en direction de l'usager, et de 128 kbit/s, en direction du réseau.

ATM (mode transfert asynchrone)/Relais de trames

Une technologie réseau souple de multiplexage et de commutation offrant une largeur de bande variable aux réseaux locaux (LAN) et longue distance (WAN).Contrairement aux configurations synchrones ordinaires, ATM permet l'attribution flexible de la largeur de bande disponible pour la transmission de données, de la voix et d'images vidéo. ATM utilise une architecture évolutive, ce qui facilite sa mise à niveau. Ce mode permet à un nombre virtuellement illimité d'usagers d'utiliser des liaisons haute vitesse spécialisées raccordées à des serveurs réseau à haut rendement. Des études d'ingénierie indiquent que ATM peut, en théorie, prendre en charge des débits de 622 Mbit/s sur fibre optique et de 155 Mbit/s sur fil de cuivre classique.

« Boîte noire »
Dispositif que les fournisseurs de services Internet (FSI) installent sur leurs serveurs pour envoyer à un organisme de sécurité gouvernemental une copie des données transmises par leur système.

Carte intelligente
Petit dispositif électronique, ayant à peu près la taille d'une carte de crédit, qui contient une mémoire électronique et parfois un circuit intégré. Les cartes contenant un circuit intégré sont également appelées *cartes de circuits intégrés (CCI)*.
Les cartes intelligentes sont utilisées dans différentes applications, telles que :

> stockage des informations médicales d'un patient ;
> argent électronique ;
> génération d'identificateurs de réseau.

CDMA (accès multiple à répartition par codes)
Technologie de transmission utilisée avec les services numériques sans fil pour transmettre la voix ou les données. Cette technologie, basée sur un procédé d'étalement du spectre, est de plus en plus utilisée partout dans le monde. La société Datang a mis au point une version chinoise de cette technologie, appelée TD-SCDMA.

Compression (algorithme)
La compression est un procédé qui permet de diminuer la taille d'un fichier ou d'un train de données afin d'accroître la vitesse de transmission ou de réduire l'espace de stockage.
Un algorithme est une formule ou une séquence d'instructions utilisée pour résoudre un problème particulier. Il est constitué d'un ensemble de règles non ambiguës qui aboutissent à un résultat clairement défini.
Une recette de gâteau, par exemple, est un algorithme. La conception d'algorithmes efficaces, c'est-à-dire simples et comportant le moins d'étapes possible, est un des principaux défis de la programmation.

Contrefaçon d'adresses IP
Technique qui permet d'accéder à un ordinateur en envoyant des données identifiées par une fausse adresse IP qui semble être celle d'un système sûr. Pour ce faire, un pirate informatique utilise une des nombreuses techniques à sa disposition pour trouver l'adresse IP d'un système sûr, puis tromper l'ordinateur en remplaçant l'adresse d'origine par l'adresse « sûre » dans les en-têtes des paquets. Les nouvelles configurations de coupe-feu et les nouveaux routeurs offrent maintenant une protection contre ce type de contrefaçon.

Convergence
Fusion d'au moins deux disciplines ou technologies distinctes. Par exemple, le télécopieur a vu le jour grâce à trois technologies convergentes, les télécommunications, le balayage optique et l'impression. D'une façon plus générale, la convergence désigne la rencontre de la télévision, de l'ordinateur personnel et d'Internet pour constituer ce qu'il est convenu d'appeler « les nouveaux médias ».

Courrier poubelle (pourriel)
Courriel non sollicité transmis à un grand nombre de destinations.

Diffusion multimédia en temps réel
Technique de transfert de données qui permet de transmettre des données en un flux continu à un débit constant. Avec la croissance d'Internet, les technologies de diffusion en temps réel jouent un rôle de plus en plus important, car la plupart des utilisateurs ne disposent pas d'une connexion permettant de transmettre rapidement des fichiers multimédias de grande taille. Grâce à la diffusion en temps réel, le navigateur ou le module complémentaire client peut commencer à afficher les données avant que le fichier ne soit complètement transmis.

Dispositif coupe-feu
Système permettant d'empêcher des personnes non autorisées d'accéder à un réseau ou de transmettre des données à l'extérieur d'un réseau. Les dispositifs coupe-feu peuvent être du type matériel ou logiciel ou une combinaison des deux, et ils sont souvent utilisés pour bloquer l'accès à des réseaux privés reliés à Internet, notamment les intranets. Toutes les communications qui pénètrent l'intranet ou qui en sortent sont analysées par le dispositif coupe-feu, qui bloque celles qui ne respectent pas les règles définies. Il existe plusieurs types de dispositifs coupe-feu :

> **Filtrage de paquets :** Le dispositif coupe-feu analyse tous les paquets qui pénètrent dans le réseau ou qui en sortent et les accepte ou les rejette en se basant sur des règles définies par l'utilisateur. Le filtrage des paquets est un système efficace et transparent pour l'utilisateur, bien qu'il soit difficile à configurer. En outre, il est très vulnérable aux procédés de contrefaçon d'adresses IP.
> **Passerelle d'application :** Applique des mécanismes de sécurité à certaines applications, comme les serveurs FTP et Telnet. Cette méthode est très efficace, mais elle réduit la performance du système.
> **Serveur mandataire :** Intercepte toutes les communications qui pénètrent dans le réseau ou qui en sortent. Ce type de serveur cache efficacement les adresses réseau réelles.

En pratique, il n'est pas rare que les dispositifs coupe-feu utilisent deux ou plus de deux méthodes de protection. Le dispositif coupe-feu est la première ligne de défense pour la protection des informations confidentielles. Au besoin, il est possible de chiffrer les données pour augmenter le niveau de sécurité.

Égal à égal
Type de réseau dans lequel chaque ordinateur possède les mêmes capacités et responsabilités. Ce type de réseau est très différent d'une architecture client-serveur dans laquelle la fonction de certains ordinateurs est strictement de desservir d'autres ordinateurs. Les réseaux d'égal à égal sont en général de configuration plus simple mais ils n'offrent pas la même performance système pour les grands volumes de trafic sur large bande.

Fibre optique
Dispositif utilisé pour transmettre des communications au moyen de fibres souples pouvant transmettre la lumière.

Filtrage des paquets
Procédé permettant de contrôler l'accès à un réseau qui consiste à analyser les paquets entrants et sortants et à laisser passer ou à bloquer des paquets en se basant sur les adresses IP (protocole Internet) du point d'origine et de la destination. Le filtrage des paquets est l'une des techniques utilisées pour créer des dispositifs coupe-feu.

paquets est l'une des techniques utilisées pour créer des dispositifs coupe-feu.

Gbit/s

Gigabit par seconde. Unité de mesure de la vitesse de transmission des données représentant 1 000 000 000 de bits par seconde. Cette unité est utilisée, par exemple, pour les réseaux à grande vitesse, tels qu'Ethernet gigabit.

Immeubles intelligents

Les immeubles intelligents sont munis de dispositifs électroniques qui prennent en charge :

> la consommation d'énergie ;
> les dispositifs de sécurité ;
> les systèmes de télécommunication ;
> l'automatisation des lieux de travail.

L'objectif ultime est de concevoir un immeuble intelligent qui réunit les quatre grandes fonctions de gestion électronique de l'immeuble en un seul système informatisé intégré, basé sur le logiciel et le matériel d'un fournisseur unique.

IP

Acronyme qui signifie *protocole Internet*. Ce protocole spécifie le format des paquets, parfois appelés datagrammes, ainsi que le mode d'adressage. La plupart des réseaux combinent le protocole IP avec un protocole de plus haut niveau, appelé TCP (*Transmission Control Protocol – Protocole de contrôle de transmission*), qui établit une connexion virtuelle entre un point d'origine et une destination.

Le protocole IP fonctionne un peu comme le système postal. Il permet d'attribuer une adresse à un message, puis de le mettre à la poste, sans qu'il soit nécessaire d'établir un lien direct entre l'expéditeur et le destinataire. Par contre, le protocole TCP/IP établit une connexion entre deux points, qui peuvent alors échanger des messages. La version actuelle du protocole Internet est *IPv4*. Une nouvelle version, appelée *IPv6*, est en cours de développement.

Large bande

Se dit d'un service utilisant une plage de fréquences étendue et pouvant fournir simultanément plusieurs voies de communications. La fibre optique, par exemple, offre beaucoup de largeur de bande.

Largeur de bande

Largeur de la plage de fréquences d'une voie de transmission. Ce terme est souvent utilisé pour désigner la quantité de données pouvant être transmise par un circuit. Plus la largeur de bande est grande, plus la quantité de données pouvant être transmise pendant une durée déterminée est grande.

Quel volume de données peut-on transmettre par une connexion ? Ce volume est généralement exprimé en bits par seconde. Par exemple, une page de texte nécessite environ 16 000 bits. Un modem rapide peut transmettre environ 15 000 bits par seconde. La transmission d'images vidéo animées exige environ 10 000 000 de bits par seconde, selon le type de compression.

Mbit/s

Mégabit par seconde (million de bits par seconde). Unité utilisée pour mesurer la vitesse de transmission des données. La vitesse des réseaux modernes, par exemple, est généralement supérieure à un mégabit par seconde.

Mux (multiplexeur)

Dispositif permettant de combiner des signaux multiples (analogiques ou numériques) et de les acheminer sur un circuit de transmission. Par exemple, un type de multiplexage très répandu combine plusieurs signaux à basse vitesse et les achemine sur une seule ligne de transmission à grande vitesse.

Passerelle

Une passerelle, également appelée *logiciel mandataire*, est un programme d'application tournant sur un dispositif coupe-feu installé entre deux réseaux. Lorsqu'un client veut établir une connexion avec une destination, il établit d'abord la connexion avec la passerelle, puis négocie avec celle-ci pour communiquer avec la destination. La passerelle établit ensuite la connexion avec la destination derrière le coupe-feu et agit au nom du client, cachant et protégeant les ordinateurs du réseau derrière le coupe-feu.Cette méthode établit donc deux connexions, l'une entre le client et la passerelle, l'autre entre la passerelle et la destination réseau. Lorsque la connexion est établie, la passerelle prend en charge l'acheminement des paquets. Puisque toutes les communications passent par la passerelle, les ordinateurs qui se trouvent derrière le coupe-feu sont protégés. Ce procédé est considéré comme très sûr, mais il exige beaucoup plus de ressources de processeur et de mémoire que les autres types de coupe-feu.

sûr, mais il exige beaucoup plus de ressources de processeur et de mémoire que les autres types de coupe-feu.

Qualité télécommunicateur
Terme qui désigne des équipements réseau offrant le niveau de fiabilité élevé requis par les fournisseurs de services Internet (FSI). L'équipement de qualité télécommunicateur affiche des pourcentages de fiabilité de 99,999 % et plus.

Réseau intranet, réseau national ou réseau à l'échelle de la Chine
Réseau privé utilisant les mêmes logiciels que le réseau Internet public mais réservé à l'usage d'une entreprise ou d'un organisme. En raison de la popularité croissante d'Internet, plusieurs outils internetisés sont maintenant utilisés dans les réseaux privés. En outre, bon nombre d'entreprises disposent maintenant de serveurs Web réservés à l'usage de leur personnel.

Réseau
Système composé de deux ordinateurs ou plus reliés les uns aux autres. Il existe plusieurs types de réseau, notamment :

> **Réseau local (RL ou LAN) :** Les ordinateurs sont relativement près les uns des autres, par exemple, dans le même immeuble.
> **Réseau longue distance (RLD ou WAN) :** Les ordinateurs sont plus éloignés les uns des autres et sont reliés par des lignes téléphoniques ou des câbles de fibres optiques.

En plus des types de réseau, certaines autres caractéristiques sont utilisées pour classer les réseaux :

> **Topologie :** La configuration géométrique des connexions qui relient les ordinateurs entre eux (bus, étoile, anneau, etc.).
> **Protocole :** Le protocole définit un certain nombre de règles et de signaux qui permettent aux ordinateurs de communiquer entre eux sur un réseau. Un des protocoles les plus courants porte le nom d'*Ethernet*. Le protocole *Anneau à jetons d'IBM* est un autre protocole souvent utilisé pour relier les PC.
> **Architecture :** Les réseaux peuvent être classés selon leur architecture, qui peut être du type *égal à égal* ou *client-serveur*.

Les ordinateurs d'un réseau sont parfois appelés *nœuds*. Les ordinateurs et les dispositifs qui fournissent des ressources à un réseau sont appelés *serveurs*.

Réseau principal
Ligne ou série de connexions constituant une voie de transmission principale dans un réseau. Toutefois, cette notion est relative, car la voie principale d'un petit réseau sera probablement d'une taille de beaucoup inférieure à celle de certaines voies secondaires dans un grand réseau.

RPV (réseau privé virtuel)
Réseau privé qui utilise le réseau téléphonique public pour relier des ordinateurs en réseau. Par exemple, bon nombre de systèmes permettent de créer un réseau en utilisant Internet pour transporter les données. Ces systèmes utilisent le chiffrement et d'autres mesures de sécurité pour empêcher des personnes non autorisées d'accéder au réseau ou d'intercepter les données.

Serveur mandataire
Serveur situé entre une application client, comme un navigateur Web, et un serveur réel. Le serveur mandataire intercepte toutes les demandes dirigées vers le serveur réel et les lui transmet, si possible, ou y répond lui-même.

TCP/IP
Acronyme signifiant *protocole de contrôle de transmission/protocole Internet*, un ensemble de protocoles de communication utilisés pour relier des ordinateurs à Internet. Le protocole TCP/IP comprend plusieurs protocoles, dont les principaux sont TCP et IP. Le protocole TCP/IP est intégré au système d'exploitation UNIX et est utilisé sur Internet, ce qui en fait la norme de facto pour la transmission des données sur les réseaux. Même les systèmes d'exploitation réseau qui utilisent leurs propres protocoles sont compatibles avec le protocole TCP/IP.

Télécommunicateur
Entreprise de télécommunications qui revend des services de communications à d'autres entreprises.

Traitement des paquets
Un paquet est un groupe de données transmis au moyen d'un réseau de commutation de paquets. En plus des données, un paquet contient l'adresse de sa destination. Dans les réseaux IP, les paquets sont souvent appelés *datagrammes*.

Notes en fin d'ouvrage

[1] HONG KONG IS SWALLOWED UP, de Jeff Jacoby, *The Boston Globe*: http://www.bigeye.com/jj070197.htm
CHINESE CHECKERS, OxBlood Ruffin, CDC
http://www.cultdeadcow.com/cDc_files/cDc-0361.html
The Money Trap, une recension de Robert Kagan
Réimpression avec la permission de *The New Republic*
Première publication le 7 avril 1997
http://www.ceip.org/people/kagrep1.htm

[2] Voir la note 59.

[3] http://www.hrw.org/backgrounder/asia/china-bck-0701.htm. Freedom of Expression and the Internet in China, A Human Rights Watch Backgrounder

[4] Dr Hsu citant un sondage de l'Académie chinoise des sciences sociales (CASS) – Dr Guo Liang, *China Academy of Social Sciences*, mai 2001

[5] (CHINANET, CHINGBN, CERNET, CSTNET et UNINET)
[Voir diagramme 1 : Un nouveau modèle pour Internet : l'innovation à l'extrémité du réseau.]

[6] Traduction de « *churukou xindao* »

[7] Voir, par exemple, http://www.wirednews.com/wired/5.06/china_pr.html
5.06 – Juin 1997, *The Great Firewall of China*, Geremie R. Barme et Sang Ye

[8] Big Brother Incorporated, Privacy International:http://www.privacy.org/pi/reports/

[9] http://www.cpsr.org/alert/cpsr.alert.2.05.html. Volume 2.05, 12 novembre 1993, publié par Computer Professionals for Social Responsibility
Washington Office
(Alert@washofc.cpsr.org)
Documents « Operation Root Canal » publiés : Questions Raised about FBI's Digital Telephony Initiative
« In response to a CPSR Freedom of Information Act lawsuit, the FBI this week released 185 pages of documents concerning the Bureau's Digital Telephony Initiative, code-named Operation "Root Canal." The newly disclosed material raises serious doubts as to the accuracy of the FBI's claim that advances in telecommunications technology have hampered law enforcement efforts to execute court-authorized wiretaps. »

[10] Source :
http://www.nortelnetworks.com/products/01/dms-10/dms10news/august99/article6.html.
Nortel a depuis retiré cette URL de son site Web. Toutefois, une copie de la page d'origine demeure dans la cache Web deGoogle. On peut la consulter à :
http://www.google.com/search?q=cache:ljjs4pWPJ8Y:www.nortelnetworks.com/products/01/dms-10/dms10news/august99/article6.html.
« Nortel has been actively involved in ad hoc committees established prior to the law being enacted. We have been active participants during the standards process with technical representatives at key meetings. »

[11] Version finale du projet de loi adopté par les deux assemblées législatives :
http://thomas.loc.gov/cgi-bin/query/z?c103:H.R.4922.ENR:H.R.4922
To amend title 18, US Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other...

[12] *Ibid*, texte tiré de la CALEA

[13] http://www.askcalea.net/about/doj990914.htm
Department of Justice and FBI Reach First Agreement Under Communications Assistance for Law Enforcement Act

[14] http://www.askcalea.com/about/pl103414.htm
« (1) IN GENERAL- A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify. »

[15] http://www.bc.edu/bc_org/avp/law/st_org/iptf/headlines/content/1997013101.html
1997 B.C. Intell.Prop. & Tech. F. 013101
Government Tempers Electronic Surveillance Proposal; Critics Laud Changes But Are Not Satisfied
par Adam White Scoville, rédacteur
Voir aussi : http://www.cdt.org/publications/pp_3.01.html
CDT POLICY POST Volume 3, Numéro 1, 17 janvier 1997

[16] Voir échéancier ENFOPOL : http://www.heise.de/tp/english/special/enfo/6382/1.html
Voir aussi : UE *Document 496Y1104(01)*
http://europa.eu.int/eur-lex/fr/lif/dat/1996/fr_496Y1104_01.html
« considérant que, selon une décision prise par les ministres "TREVI" en décembre 1991, une étude devrait être effectuée en ce qui concerne les conséquences de l'évolution juridique et technique et de l'évolution du marché dans le domaine des télécommunications à l'égard des différentes possibilités d'interception et en ce qui concerne les mesures à prendre afin de faire face aux problèmes qui ont surgi... »

[17] Pour obtenir le texte intégral de tous les documents ENFOPOL cités dans le présent document, rendez-vous à http://www.statewatch.org/eufbi/index.html.
A sa première réunion à Bruxelles les 29 et 30 novembre 1993, le nouveau Conseil des ministres de la Justice et de l'Intérieur a adopté la résolution suivante sur l'interception des communications. Elle parle d'elle-même et est reproduite en entier ici en anglais:
« RÉSOLUTION DU CONSEIL SUR L'INTERCEPTION DES TÉLÉCOMMUNICATIONS
Le Conseil
1. demande au groupe d'experts de comparer les besoins des États membres de l'Union à ceux du FBI;
2. convient que, pour éviter un débat axé uniquement sur les besoins du FBI, ceux des États membres de l'Union seront communiqués aux pays tiers qui ont participé à la réunion du FBI à Quantico (notamment la Suisse, la Norvège, la Finlande [pays ayant fait une demande d'accession à la Communauté européenne], les États-Unis et le Canada) et qui sont mentionnés dans le protocole approuvé par les ministres lors de leur réunion tenue à Copenhague;
3. approuve pour des raisons pratiques que la décision sur la coopération des pays tiers prise à la réunion des ministres à Copenhague s'applique également à Hong Kong, à l'Australie et à la Nouvelle-Zélande (ayant participé à la réunion du FBI);
4. par les présentes décide que des discussions non officielles avec les pays précités peuvent être envisagées : à cette fin, la présidence et le groupe d'experts peuvent, par exemple, organiser une rencontre avec ces pays tiers pour échanger de l'information. »

[18] Voir www.europarl.eu.int/stoa/publi/pdf/981401-5en_en.pdf:
SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT
STOA
DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE
OF ECONOMIC INFORMATION
Vol.5/5: The perception of economic risks arising from the potential vulnerability of
electronic commercial media to interception

[19] http://www.oneworld.org/index_oc/issue198/codewar.html: The code war
David Banisar et Simon Davies. David Banisar est un avocat du Electronic Privacy Information Center (EPIC) à Washington, DC, directeur adjoint de Privacy International (PI) et coauteur d'un nouveau livre sur la politique de chiffrement: *The Electronic Privacy Papers: The Battle for Privacy in the Age of Surveillance*. Simon Davies est directeur général de PI, auteur de *Big Brother* et visiteur stagiaire de la London School of Economics.

[20] www.europarl.eu.int/stoa/publi/pdf/981401-5en_en.pdf

[21] http://www.statewatch.org/eufbi/index.html

[22] Draft COUNCIL RESOLUTION on the lawful interception of telecommunications in relation to new technologies ENFOPOL 19, 15 mars 1999 : http://www.fipr.org/polarch/enfopol19.html

[23] What do YOU want the Internet to be? http://www.nortelnetworks.com/corporate/internet/what_do_you_want/index.html

[24] China looks for new technology to police Net
par Martin Fackler, Associated Press, 9 novembre 2000

[25] http://www.adsaleexh.com/sec/press2.html
Communiqué, 29 août 2000
Over 300 International Exhibitors Gather in Security China 2000
Taping the Lucrative China Market

[26] *Ibid*

[27] http://www.adsaleexh.com/sec/press1.htmmime text/html
Communiqué, 10 mars 2000
The No. 1 International Security Exhibition back to Beijing again

[28] *Ibid*, Adsale

[29] *Ibid*, Adsale

[30] Research Overview, Speech Signal Processing and Intelligence Technology Group Department of Electronic Engineering, Tsinghua University
http://www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm
Tsinghua a depuis retiré cette URL de son site Web. Toutefois, une copie de la page d'origine demeure dans la cache Web de Google. On peut la consulter à :
http://www.google.com/search?q=cache:4Ew-AlksjbU:www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm+863+tsinghua+engineering+speech+continuous&hl=en

[31] *Ibid*

[32] http://www.most.gov.cn/English/Programs/863/menu.htm

[33] http://138.110.28.9/acad/intrel/chinmc.htm
EVAN A. FEIGENBAUM, China's Military-Civilian Complex, *New York Times*, 22 mai 1998

[34] *Ibid*, 27

[35] *Ibid*

[36] BNR exploite des laboratoires de recherche dans plusieurs pays, notamment deux au Canada (Ottawa et Montréal), trois aux États-Unis (Raleigh, Richardson et Atlanta), quatre au Royaume-Uni (Harlow, New Southgate, Maidenhead etMonkstown), un au Japon (Tokyo), un en Australie (Sydney) et un en Chine (Beijing).

[37] Nortel Networks signe des contrats évalués à plus de 120 millions de dollars US pendant la visite du premier ministre Jean Chrétien en Chine.
http://www.nortelnetworks.com/corporate/news/newsreleases/1998c/11_20_9898638_Chretien.html

[38] http://www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm

[39] Objectifs précis de conformité - J-STD-025 établit les normes pour la conformité de base à la CALEA :
voir Plate-forme série DMS-500 de Nortel, Document no : 51047-16-12-00.pdf.

[40] http://www.nortelnetworks.com/corporate/news/newsreleases/1998c/11_20_9898638_Chretien.html

[41] Plus de 100 millions $US dans le cas de Nortel selon le Département de la justice américain : voir www.doj.gov.

[42] http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[43] Selon un rapport du 12 juin dans le quotidien *China Daily*.

[44] http://www.smartcards-china.com/en/page_ehydt1.htm[45]
http://www.state.gov/www/global/human_rights/1999_hrp_report/china.html
Site FTP pour information du *Department of State*, avant le 20 janvier 2001.
1999 Country Reports on Human Rights Practices
Publié par le Bureau of Democracy, Human Rights, and Labor
U.S. Department of State, 25 février 2000

[46] Signalé à Mingbao, information fournie par Judy Chen, HRIC

[47] http://www.telecomn.com/english/china_comm/CN_200010.htm *DATANG TELECOM CONTRACTS "INTELLIGENT BUILDING WEAK CURRENT ENGINEERING" FOR JILIN PROVINCIAL PUBLIC SECURITY DEPARTMENT*

[48] http://www.gzjd.gov.cn/gzjd/

[49] *Ibid*, AP

[50] China Online, http://www.chinaonline.com/topstories/001114/1/c00111456.asp

[51] http://www.nortelnetworks.com/corporate/events/2001b/myviewtour/plenary_fr.html

[52] « The idea that ISPs are watching where [customers] go is unacceptable… it's like the Post Office looking into your mail in order to decide what kind of junk to send you. » (Junkbusters.org) Plusieurs projets de loi sur la vie privée sont actuellement en cours d'introduction ou de réintroduction au Congrès des États-Unis et autres corps législatifs des États-Unis. Un des projets de loi à l'étude au Congrès, la Spyware Control and Privacy Protection Act, vise à protéger les utilisateurs en ligne contre la technologie Internet Personnel de Nortel. Évidemment, en Chine, le polluriel et le télémarketing sont les derniers des soucis.

[53] En plus d'OPTera Metro, la solution de Nortel pour Shanghai Telecom comprend le Shasta 5000 Broadband Service Node (BSN) et les autocommutateurs multiservices Passport 15000 et Passport 7480 de Nortel Networks.

[54] http://www.nortelnetworks.com/help/legal/index_fr.html#privacy

[55] *Ibid*

[56] AN APPRAISAL OF THE TECHNOLOGIES OF POLITICAL CONTROL, An Omega Foundation Summary & Options Report For The European Parliament, septembre 1998

[57] *Ibid* 22 (AP)

[58] (Voir Norris, C., et. al, 1998.)

[59] Nexus (www.nxsgrp.com et www.nxs.ca), anciennement Heritage Concepts International (HCI). NEXUS Group International Inc. AND Corporation (www.andcorporation.com). AcSys Biometrics Corp. (www.acsysbiometricscorp.com).

[60] http://www.andcorporation.com/press/press_3_12_01.html. AcSys Biometrics Accompanies Nortel Networks to CeBIT 2001

[61] Bob Paquin, article sur le site Web du journal *The Ottawa Citizen*, lundi 26 octobre 1998, E-Guerillas in the mist.

[62] Linux World Conference:http://www.linuxworld.com/

[63] http://www.cultdeadcow.com/cDc_files/declaration.html

« Si vous vous tenez toujours droit,
alors votre ombre ne sera jamais courbée. »
> Liu Qing, ancien prisonnier politique

Autres publications de Droits et Démocratie :
(Consultez notre site www.ichrdd.ca pour une liste complète de nos publications.)
Un cadre de référence des droits humains pour le commerce dans les Amériques, par Diana Bronson et Lucie Lamarche, 2001.
Le dialogue bilatéral avec la Chine affaiblit le système international de protection des droits humains, 2001.
Protection des droits humains et mondialisation de l'économie. Un défi pour l'OMC, par Robert Howse et Makau Mutua, 2000.
Les intérêts miniers canadiens et les droits de la personne en Afrique dans le cadre de la mondialisation, par Bonnie Campbell, 1999.
Les femmes et la consolidation de la paix, par Dyan Mazurana et Susan McKay, 1999.
Donner une conscience au commerce : stratégies d'intégration des droits humains aux affaires courantes des entreprises, Volume 2, par Craig Forcese, 1997.
Les droits humains : le chaînon manquant de l'APEC, 1997.

```
<html>
<head>
  <title>Droits et D&eacute;mocratie - Centre international des droits de la personne et du
d&eacute;veloppement d&eacute;mocratique</title>
<base target="contenu"></head><!- frames ->
<frameset cols="18%,82%">
<frame src="http://www.ichrdd.ca/111/navigationFrancais.html"
      name="chinas golden shield"
      frameborder="0"
    framebordercolor="e4e3ca"
      scrolling="fluto"
      noresize
      marginwidth="5"
      marginheight="5">

<frame name="contenu" src="http://www.go.openflows.org/111/page1china.html" marginwidth="5"
marginheight="5" scrolling="auto" frameborder="0" framebordercolor="e4e3ca" noresize>
</frameset>

<body link="000000" alink="000000" vlink="000000">
```

Droits et Démocratie

Centre international des droits de la personne
et du développement démocratique

1001, boul. de Maisonneuve Est, Bureau 1100 > Montréal (Québec) H2L 4P9
Tél. : 1 (514) 283-6073 > Téléc. : 1 (514) 283-3792 > Courriel : ichrdd@ichrdd.ca > Site Web : www.ichrdd.ca