SCOTT CHARNEY

Vice président de Trustworthy Computing, Microsoft

Jim HOAGLAND, Associate Editor, Chief Foreign Correspondent of the *Washington Post*

Je pense que ceci est un élément de réponse que nous allons pouvoir développer. Il s'agit ici d'essayer d'identifier, dans les domaines de ces nouvelles technologies, ce qui peut être fait précisément par des organismes internationaux en matière de gouvernance mondiale pour prévenir ce genre de catastrophe.

Je souhaiterais maintenant que nous discutions de la technologie de la cybersécurité et du cyberespace. Je dois vous avouer que je suis un peu plus intéressé par le sujet depuis cette semaine, parce que j'ai été victime pour la première fois de ma vie d'un vol d'identité par Internet. Et je pense que j'ai rejoins une grande cohorte. Pourriez-vous nous expliquer, Scott, ce qu'est le « trustworthy computing », le rôle de Microsoft dans ce domaine, et de quelle façon vous analysez les menaces qui pèsent sur la sécurité informatique ?

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

Tout d'abord, permettez-moi de dire qu'il est vraiment passionnant de participer à un débat qui met en relation la technologie et le nucléaire. La technologie continue à m'étonner, dans le sens où elle touche presque toutes les facettes de la société humaine. Le programme « Trustworthy-Computing » de Microsoft était de créer des logiciels sécurisés, respectueux de la vie privée et fiables. Notre président Bill Gates en a été l'initiateur il y a 10 ans environ et nous commémorons d'ailleurs le 10e anniversaire de sa création le 15 janvier 2012. Son principe était le suivant : si la technologie devait être incorporée avec succès dans toutes les facettes de la vie, elle devait être sécurisée, respectueuse de la vie privée et avoir un niveau de fiabilité aussi élevé que celui de l'énergie et du téléphone. Cependant, bien sûr, cette technologie n'était pas tout cela.

On constate qu'il y a en réalité quelques parallèles intéressants avec le nucléaire. Tout d'abord, l'Internet a été conçu avant tout pour résister aux attaques nucléaires. C'est la raison pour laquelle il a été conçu par l'armée américaine. Son prédécesseur, l'Advanced Research Projects Agency Network (ARPANET), a été conçu pour que, dans le cas où une ville serait rasée par une bombe nucléaire, on puisse maintenir les communications en contournant la zone touchée. Quarante ans plus tard, il s'avère que des logiciels sont utilisés pour paralyser les centrifugeuses d'une usine qui produit de la matière nucléaire. Ils sont créés pour éviter une attaque nucléaire et servent à éviter potentiellement la prolifération nucléaire.

L'autre point intéressant est que, si un événement cataclysmique quelconque se produit, il apparaît de plus en plus évident que l'internet contribuera majoritairement au processus de réponse . La raison en est que dans tous les cas de désastres majeurs aujourd'hui, tel que l'ouragan Katrina ou le séisme de mars 2011 au Japon, les deux réseaux, filaire et cellulaire, sont très rapidement saturés. De plus, les réseaux traditionnels permettent aux premiers intervenants d'assurer des communications vocales, mais l'Internet offre un plus grand éventail de possibilités.

Quand l'Ouragan Katrina a frappé les États-Unis, il y a eu une inondation si importante dans la ville de la Nouvelle-Orléans que beaucoup de panneaux de signalisation étaient sous l'eau. Les gens qui essayaient de faire quelque chose, même en bateau, ne savaient pas où ils se trouvaient. On a compris alors que les téléphones portables ne suffisaient pas, et que si les gens avaient emporté un Smartphone, ils auraient pu non seulement être en

communication vocale, mais aussi transmettre des données et utiliser des services de cartographie et de géolocalisation GPS. Du coup, les premiers intervenants qui réagissent à une catastrophe pourraient vérifier leur position sur un appareil portatif, par rapport à leur environnement, et donc bénéficier de plusieurs types de communication sur un appareil unique.

L'Internet va jouer un rôle énorme dans la protection des personnes pendant les cataclysmes. Il va également jouer un rôle très important dans notre réflexion sur la façon de nous adapter à toutes ces nouvelles crises. Un autre point important, à mon sens, est qu'il y a eu une profusion de discours ces dernières années sur la possible mise hors service de l'Internet par les terroristes. À mon avis, il s'agit d'un battage médiatique qui n'est pas étayé par les faits. D'abord, l'Internet n'est pas un seul réseau; il s'agit plutôt d'un réseau de réseaux. Et les organisations terroristes utilisent l'Internet elles aussi pour leurs communications, collectes de fonds et toutes sortes d'autres opérations.

Ensuite, il est très difficile, dans la réalité, de détraquer un système comme l'Internet parce qu'il est diffusé massivement et n'est régi par aucune autorité centrale. Cela ne signifie pas que des organisations n'attaqueront pas certaines parties de l'Internet comme le système bancaire, le réseau électrique ou d'autres sous-ensembles, afin de causer des dommages. Je conclurai mes observations préliminaires en disant que l'Internet représente évidemment un grand défi. Il y a en effet sur Internet beaucoup d'acteurs différents animés par des motifs différents. Il y a des cybercriminels, des organisations terroristes, des États-nations engagés dans le cyberespionnage et, potentiellement, dans la cyberguerre. Le problème est le suivant : malgré la diversité de tous ces acteurs et la diversité de ce qui les motive, leurs attaques se ressemblent, car les bits restent des bits et les paquets de données restent des paquets.

D'après les critères du monde traditionnel d'antan, si quelqu'un cambriole une banque, je peux vous dire qu'il s'agit probablement d'un criminel motivé par l'argent. Si un avion de combat abat un avion de ligne civil, ce qui est arrivé il y a des années, vous savez qu'il s'agit de l'action d'un État-nation parce que les civils n'ont pas accès aux avions de combat. En revanche, n'importe qui a accès à l'informatique et à l'Internet. Se pose donc un problème de guerre asymétrique, car il est extrêmement difficile de savoir d'où vient l'agression. Une attaque subie par un gouvernement ou une banque par déni de service pourrait résulter d'une activité organisée, d'un acte solitaire ou encore de l'activité d'un État-nation. Il est donc très difficile de savoir à qui en attribuer la responsabilité.

Jim HOAGLAND, Associate Editor, Chief Foreign Correspondent of the *Washington Post*

Scott, Monsieur le Directeur Général Amano a dû faire face à un véritable cauchemar cette année à Fukushima. Pouvez-vous nous décrire quel est votre cauchemar à vous dans le monde virtuel ? Quel désastre serait plausible en théorie, mais quasi inimaginable en pratique, à l'heure actuelle ?

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

Je pense qu'il faut absolument que les gens commencent à mieux comprendre à quel point l'Internet relie désormais la vie de chacun de nous. C'est notre tissu social. Quand les ordinateurs individuels sont arrivés, l'idée était qu'il y aurait un ordinateur sur chaque bureau. Chaque logement et chaque bureau devait être équipés d'un ordinateur et c'est exactement ce qui s'est passé, mais grâce à la pression des entreprises pour augmenter la productivité du travail.

Aujourd'hui, bien sûr, les gens ont recours aux technologies de la communication en permanence et dans tous les domaines de leur vie. Vous pouvez le constater, par exemple, avec les printemps arabes. Le résultat, c'est que nous avons supprimé les systèmes qui assuraient l'activité humaine normale en cas d'indisponibilité des machines. Par exemple, si vous sollicitez des services médicaux et que les ordinateurs sont inopérants, il n'y aura aucune trace papier.

Je vais vous donner un exemple tiré de la réalité. Je participais à un groupe de travail du Conseil consultatif des sciences appliquées à la Défense sur le thème de l'assurance logicielle aux États-Unis. Bon nombre de gouvernements dans le monde, qui possèdent des armées sophistiquées, utilisent un système apparenté au « Blue-Force Tracking» (suivi en temps réel des positions amies). En substance, chaque pièce d'équipement et toutes vos forces sont dotées de puces électroniques; une couleur est attribuée à chaque groupe, que vous pouvez visualiser sur des cartes. Le rouge représente les forces ennemies, et le bleu les forces amies. Un jour, quelqu'un m'a dit : « Vous savez, la pire des choses qui pourrait arriver, c'est que quelqu'un puisse intervertir les couleurs.» J'ai répondu, « En fait, ce n'est pas le pire des scénarios, parce que vous ne tuerez vos hommes qu'une fois. Mais c'est comme ça que vous saurez que vos données sont erronées.»

Le problème qui se pose, c'est l'absence de jumelles. Si vous vous en rappelez, dans les vieux films sur la Seconde Guerre mondiale, les généraux montaient en haut des collines avec leurs jumelles et pouvaient vérifier la position de chacun. Le problème est qu'actuellement plus personne n'est équipé de jumelles, et nous nous trouvons dans une situation analogue à celle évoquée tout à l'heure où les professionnels de la santé ne disposent plus de dossiers/documents papier. Nous sommes devenus totalement dépendants de la technologie sans pour autant entretenir des systèmes de secours. Quel serait alors le scénario catastrophe ? Si le réseau électrique ne fonctionne plus, tout le reste tombe en panne. Si le système de télécommunication ne fonctionne plus, il y a un effet en cascade sur les banques. Et bien d'autres effets.