DÉBAT

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

Je me permets de revenir sur le point que vous avez mentionné plus tôt, et qui mérite vraiment que l'on s'y arrête. C'est celui du danger de l'attaque d'une centrale nucléaire par l'informatique. Monsieur Amano, pourriez-vous nous dire ce que fait votre agence (l'AIEA) pour prévenir ce type de danger ? Est-ce un sujet sur lequel vous travaillez activement ou ce domaine est-il uniquement du ressort des gouvernements nationaux ? Et, si vous le savez, que font les gouvernements nationaux pour protéger les centrales nucléaires ?

Yukiya AMANO, Directeur général de l'AIEA

Nous agissons dans ce domaine. Nous formons des gens à combattre les attaques cybernétiques visant des centrales nucléaires. Nous sommes conscients qu'elles représentent un des dangers potentiels pour ces installations.

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

Formez-vous le personnel des centrales ou votre propre personnel ?

Yukiya AMANO, Directeur général de l'AIEA

Bien sûr, nous formons notre propre personnel et celui des États membres, qu'il s'agisse d'experts gouvernementaux ou de personnes travaillant dans ce domaine. Parfois, ce sont des collaborateurs de sociétés privées. Nous organisons des réunions de formation pour les préparer aux attaques cybernétiques. Cependant, c'est un champ tout nouveau et nous devons faire des efforts supplémentaires pour préparer les gens à ces éventualités et aux dangers qu'elles représentent.

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

Quelle éventualité craignez-vous le plus, dans le cas d'une attaque cybernétique contre une centrale nucléaire ? Que pourrait-il se passer?

Yukiya AMANO, Directeur général de l'AIEA

Les centrifugeuses et les installations d'enrichissement des centrales nucléaires sont très sensibles aux attaques cybernétiques. Leurs systèmes d'exploitation sont aussi très vulnérables. Dans le passé, ils étaient commandés par

des systèmes analogiques, mais actuellement la plupart des salles de commande sont informatisées. Perturber ces systèmes par des attaques cybernétiques aurait les conséquences les plus graves.

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

Scott, quelle serait votre réponse à la même question ?

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

Il y a déjà eu des preuves de telles attaques quand, par exemple, des personnes ont provoqué une surchauffe et des machines ont pris feu. Il y a eu également des cas d'attaques au cours desquelles des systèmes de commande ont été manipulés de façon non agréée ou prévue par leur propriétaire. Je pense que les remarques de Monsieur Amano sont parfaitement justes. Je voudrais cependant insister sur la nécessité de créer une structure pour réfléchir à ce que l'on redoute et pour y parer. En premier lieu, nous devons développer un modèle. Mais pour tout modèle que nous élaborons, réussi ou non, nous avons besoin d'un bon modèle de menace. Ce qui signifie que nous devons savoir ce que nous possédons et ce que nous essayons de protéger. Que ferait un acteur malveillant pour perturber mes installations ? C'est sur la base de ces modèles de menaces que nous devons mettre en place un ensemble de procédures.

Le problème, c'est qu'il s'agit toujours de *gestion* du risque, et non d'*élimination* du risque. Dans le monde physique, nous ne pouvons pas non plus éliminer les risques ; des avions continuent de s'écraser. Dans le cyberespace, la difficulté consiste à quantifier le niveau d'atténuation du risque auquel on peut parvenir en appliquant certaines procédures. Toute ma vie, j'ai eu ce problème avec les entreprises. Je pouvais leur affirmer : « Voici un ensemble de moyens de protection et voilà leur prix à l'unité. Ce prix inclut le temps de travail, le temps d'installation, et l'octroi de la licence du produit.» L'acheteur potentiel me disait alors : « Si je dépense autant d'argent, quelle sera le niveau de réduction du risque ? Est-ce que le résultat dépassera le coût de mon investissement ?» Le problème est que nous ne pouvons pas quantifier le risque cybernétique en termes de dollars. Il s'agit donc d'une décision très difficile à prendre pour des chefs d'entreprise.

Yukiya AMANO, Directeur général de l'AIEA

Je voudrais ajouter quelques mots. Lors de la gestion de l'accident de Fukushima Daiichi, la période la plus frustrante ce furent les deux ou trois premiers jours. En effet, nous avons contacté les autorités japonaises et essayé d'obtenir des informations, mais en vain, parce que tous les instruments dans les réacteurs avaient été mis hors service par le tsunami. Il y avait une panne d'électricité totale et nous ne pouvions même pas obtenir un minimum d'informations. Nous n'avions aucune idée de ce qui se passait et nous étions donc dans l'incapacité d'informer nos populations ou nos médias. Si la même chose arrivait, non pas à cause d'un tsunami, mais à cause d'une attaque cybernétique, nous serions dans la même situation, c'est à dire une situation très dangereuse.

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

Je pense que cette idée de modèles des menaces est très importante. Ce n'est pas très connu, mais je crois savoir que les centrales nucléaires américaines ont été renforcées pour pouvoir résister à un avion qui s'écraserait sur elles. Ceci est évidemment une conséquence du 11 septembre 2001. Mais je suis heureux que vous nous ayez ramenés

au thème de Fukushima, car je souhaitais continuer notre discussion sur ce sujet. Pourriez-vous nous dire si les radiations émises par la centrale représentent une menace pour d'autres pays que le Japon ?

Yukiya AMANO, Directeur général de l'AIEA

Je ne le pense pas. Quand on parle de radiations, il y deux points à souligner. Une exposition à des radiations très fortes durant une longue période et à proximité de la source est dangereuse et peut même être létale. C'est ce qui pourrait arriver sur le site de la centrale ou dans le cas d'une explosion nucléaire. On appelle cela l'effet déterministe. Loin ou hors du site, c'est à dire à environ 20, 30 ou 50 km de distance, il y a un risque d'exposition aux radiations, et rester pendant longtemps dans un tel environnement peut générer un cancer au bout de 10 ou 20 années. C'est un problème qui concerne, comme je l'ai dit, les gens se trouvant dans un rayon de 20, 30 ou 50 km.

Nous avons contrôlé les niveaux de radiations dans le monde entier et avons effectivement détecté un certain changement, mais ce changement était infime et sans aucun effet sur la santé humaine. Le corps humain est fait pour résister aux radiations qui existent partout dans la nature, y compris dans cette salle. Des radiations sont émises par les pierres, le béton, l'espace, par tout. Aussi puis-je vous assurer que les hausses de niveau de radiation causées par l'accident de Fukushima Daiichi n'ont aucun effet sur la santé humaine dans des pays éloignés.

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

Monsieur Amano, au vu de l'hystérie générale en Allemagne à la suite de la catastrophe japonaise, un ami allemand m'a confié qu'on aurait pu croire que les réacteurs étaient à Darmstadt plutôt qu'à Fukushima. Comment pouvez-vous expliquer ce comportement ?

Yukiya AMANO, Directeur général de l'AIEA

Je pense que c'est une question de confiance. Comme les radiations sont invisibles, les gens ont un symptôme psychologique de crainte qui pose un problème très sérieux. Après l'accident de Fukushima Daiichi, j'ai reçu une lettre d'une personne que je ne connaissais pas me disant qu'elle avait acheté une radio fabriquée en Chine et avait constaté plus tard qu'une pièce était faite au Japon. Elle me demandait si elle pouvait quand même l'écouter sans danger. J'ai eu envie de lui dire, « Tant que vous ne mangez pas la radio, il n'y a aucun risque ! », mais je ne l'ai pas dit.

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

Quelle menace les radiations représentent-elles au Japon? Cette question est en particulier liée au fait que les officiels japonais auraient déclaré l'impossibilité pour les habitants de retourner dans le voisinage de la centrale avant des décennies.

Yukiya AMANO, Directeur général de l'AIEA

Cela dépend de la zone concernée. Pour le préciser, nous avons dû dresser une carte de la contamination. Il y a ce que nous appelons les « hot spots » (points chauds), qui sont des zones où les niveaux de radioactivité sont

relativement élevés. Il vaut mieux ne pas y aller, ou alors seulement après la décontamination du sol. D'autre part, les niveaux de radiation sont importants dans certains aliments, mais le gouvernement s'occupe de les contrôler. Il suffit de s'arrêter de les consommer pour éviter tout effet négatif sur la santé. Quand le gouvernement met en garde au sujet d'un aliment, il est préférable de ne pas en manger.

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

Je poserai deux dernières questions sur ce sujet. Quel est selon vous l'avenir de l'énergie nucléaire au Japon ?

Yukiya AMANO, Directeur général de l'AIEA

C'est une prévision très difficile à faire et qui comporte beaucoup d'incertitudes. Il est compréhensible que les gens aient très peur. Suite à la catastrophe, les habitants dans un rayon de 20 ou 30 km ont été évacués. Et l'accident n'est pas encore terminé aujourd'hui. La construction de nouvelles centrales nucléaires me semble difficile dans ce contexte.

Cependant, nous sommes en discussion avec le gouvernement japonais, qui conduit actuellement ce que nous appelons des « tests de résistance » pour savoir si les centrales nucléaires pourraient supporter des risques naturels sérieux comme des tsunamis, des tremblements de terre ou des inondations. L'AIEA est maintenant prête à réexaminer cet aspect des choses et c'est ce que nous avons commencé à faire. Si l'exploitation des centrales nucléaires est relancée, il est préférable qu'elle le soit après que la sécurité ait été garantie par le gouvernement et peut-être vérifiée par l'AIEA.

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

C'était, en fait, ma deuxième question. Dans quel délai pensez-vous pouvoir accorder cette garantie ?

Yukiya AMANO, Directeur général de l'AIEA

Nous attendons le feu vert et c'est une démarche qui ne devrait pas prendre beaucoup de temps. Elle consiste essentiellement à élaborer un modèle informatique qui peut être terminé en quelques semaines ou quelques mois tout au plus. Si on nous donne cette possibilité, c'est réalisable assez rapidement. Nous pouvons envoyer une mission pour aider les exploitants et les autorités japonaises. Cela ne prendra pas des années; ce sera au maximum une question de semaines ou de mois.

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

Scott, je voudrais que vous nous parliez un peu du rôle que jouent les entreprises privées dans la sécurité nationale et internationale et que vous nous disiez si oui non vous jouez un rôle dans la gouvernance mondiale. J'aurais dû dire, lors de mon introduction, que Scott a longtemps été en poste dans la section de la cybercriminalité du ministère de la Justice américain. Pourriez-vous nous expliquer un peu la différence entre cybercriminalité et cyberterrorisme? Selon vous, que devraient faire les entreprises privées, les gouvernements nationaux et peut-être certaines instances internationales que vous pourriez nous aider à identifier ?

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

Du point de vue d'un modèle de gouvernance, l'Internet est un véritable défi. Les gouvernements du monde entier élaborent actuellement des stratégies de cybersécurité. Ceci est un défi très important pour une raison bien précise : en règle générale, quand un gouvernement s'attaque à des problèmes de ce niveau, il dispose souvent d'une bonne maîtrise des moyens d'action. Il y a une comparaison intéressante à faire sur ce point : pendant la guerre froide, les gouvernements avaient conçu et entretenu les armes nucléaires et ils gardaient le doigt sur la gachette. Dans cette situation, ils étaient à la fois responsables de la sécurité nationale et maîtres des moyens d'action.

L'aspect intéressant de l'Internet, c'est qu'il a été conçu, développé et, encore maintenant, entretenu à 85-90 %, par le secteur privé.Le problème de la cybercriminalité s'étant aggravé et le terrorisme et la guerre cybernétique étant devenus des préoccupations plus importantes pour les gouvernements, ceux-ci ont déclaré : « Nous avons la responsabilité, et c'est notre responsabilité traditionnelle, d'assurer la sécurité publique et la sécurité nationale, Cependant, nous n'avons pas la maîtrise de ce système. Il est conçu, développé et entretenu par le secteur privé.

De ce fait, la plupart des gouvernements à travers le monde se sont fixés comme objectif d'établir ce qu'ils appellent un partenariat public-privé. C'est un partenariat gouvernement-industrie destiné à protéger l'Internet. À dire vrai, dans les premières années de ce partenariat, les deux parties se sont trompées d'objectif. Elles se sont focalisées essentiellement sur le partage d'informations Elles partaient du principe que l'industrie était très pointue sur le fonctionnement, la vulnérabilité et les menaces potentielles du système, tandis que le gouvernement possédait beaucoup d'informations sur les adversaires. Leur théorie était la suivante : la simple mise en commun de toutes ces informations améliorerait la situation.

Malheureusement, cela n'a pas fonctionné parce que l'échange d'informations ne s'est pas fait. Les gouvernements ne partagent pas volontiers leurs informations dans le souci de protéger leurs sources et leurs méthodes, jugeant certaines informations trop sensibles pour être divulguées. De son côté, l'industrie n'est pas encline à partager ses informations pour la simple raison que révéler la vulnérabilité de ses produits n'est pas le meilleur moyen de conserver la confiance des marchés et d'accroitre sa réputation. Demeure aussi la question de savoir ce que l'on va faire de ces informations, une fois échangées.

C'est pourquoi, au fil du temps, j'en suis venu à repenser le partenariat public-privé. J'ai conçu un autre modèle que j'encourage les gouvernements à adopter. Voici l'état actuel de ma pensée. Les entreprises du secteur marchand fournissent un certain niveau de sécurité qui répond aux exigences des clients qui sont donc prêts à en payer le prix. C'est ce qu'on appelle le libre jeu des mécanismes du marché. Mais, en fait, nous allons même un peu au-delà, car nous sommes des entreprises socialement responsables et citoyennes.

Cela dit, ce ne sont pas les marchés qui fournissent la sécurité sur le plan national et public. Il est impossible d'expliquer la Guerre Froide par la loi du marché. Par conséquent, pour répondre à un besoin à ce niveau, il faut généralement mettre en œuvre un autre mécanisme, tel qu'une action gouvernementale. Conscient de cette vérité, j'ai dit aux gouvernements ma façon de voir le partenariat public-privé. Il s'agit, en l'occurrence, de comprendre quel niveau de sécurité peuvent assurer, d'un côté les mécanismes du marché et de l'autre, les fournisseurs. Puis il faut évaluer les besoins en termes de sécurité nationale et de sécurité du public, et enfin de chercher ensemble les moyens de les concilier.

Dans ce domaine, le gouvernement dispose d'un grand nombre d'outils. Faisant partie des organismes de normalisation, il a le pouvoir de fixer des normes. Dans la plupart des pays, les gouvernements sont les plus gros acheteurs de technologies de l'information. Chacune de leurs exigences d'achat régit le marché. Et ils ont le pouvoir de réglementation, si nécessaire. La véritable clé consiste à savoir comment établir ce modèle de gouvernance.

Par ailleurs, il est important de noter que l'Internet a prospéré en partie parce qu'il n'a pas de modèle de gouvernance. Personne ne gère l'Internet. Il existe seulement deux organismes : le groupe d'ingénierie Internet qui travaille sur la standardisation, et la Société Internet pour l'Assignation des Noms et des Nombres (ICANN), qui gère le système des noms de domaines. Cependant, depuis que le gouvernement américain a retiré l'Internet du domaine

militaire pour en faire une ressource publique, il a toujours été géré de façon coopérative. C'est ce qui explique le défi qu'il représente pour les gouvernements, car ceux-ci sont habitués à réfléchir aux problèmes en termes de structures de commandement et de contrôle, alors qu'il n'existe aucune structure de cette sorte pour l'Internet.

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

Comment décririez-vous la réponse des gouvernements au défi que vous venez de présenter. Prenons les cas des gouvernements américain et européens ?

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

Je pense qu'il y a eu une amélioration. Les États se sont associés pour développer des stratégies de cybersécurité cohérentes et harmonisées et ils travaillent également sur des stratégies internationales. Cela dit, ils doivent faire face à quelques énormes défis. Le premier, qui est l'immense difficulté de l'attribution d'identité sur l'Internet. Je ne vous dis pas à quel point cela est important. Sur ce point, je vais utiliser l'exemple des États-Unis, parce que j'ai passé un certain temps au ministère de la Justice de ce pays.

La plupart des gouvernements fonctionnent de la même manière. Ils craignent un certain nombre de menaces similaires. Ils craignent la criminalité. Ils craignent les réseaux de renseignement. Ils craignent la guerre. Pour chacun de ces domaines, ils ont des organismes spécialisés qui gèrent la question. Ils ont des organismes chargés de faire respecter la loi; des agences de renseignement et des institutions militaires. Ces organismes exercent différents types d'autorités. Ils ont respectivement le pouvoir judiciaire d'effectuer des écoutes téléphoniques et de réunir des preuves, le pouvoir en matière d'espionnage et la force militaire.

Le choix de l'organisme qui sera sollicité en cas de besoin est fonction de deux éléments: l'auteur de l'agression et le motif de l'attaque. Pour un acte criminel, il sera fait appel à un organisme de maintien de l'ordre et à l'autorité judiciaire ; si l'on soupçonne un vol de renseignements militaires, ce sera l'agence de renseignement et ses services qui seront mobilisés ; dans le cas d'une attaque par des bombes cinétiques, c'est l'institution militaire et l'armée qui interviendront, chaque organisme faisant autorité dans son domaine. Encore une fois, ce sont l'identité de l'agresseur et le motif de l'agression qui déterminent la réaction. Or quand il s'agit d'une attaque par l'Internet, quels sont les deux éléments que vous ignorez : c'est qui attaque et pourquoi. Vous êtes coincés.

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

Existe-t-il une réponse militaire appropriée à une attaque qui détraquerait le réseau d'électricité, ainsi que les marchés et le secteur financier d'un pays? Prenons de nouveau l'exemple des États-Unis. Que pourraient-ils faire militairement dans un tel scénario ?

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

Il y a deux terrains d'action militaire. Le premier est sans doute celui de la cyber. Elle comporte un volet défensif, qui consiste à supprimer des paquets de données, et un volet offensif, qui consiste à tirer des paquets en retour. Cependant, on peut également lancer des actions. Un des problèmes spécifiques du cyberespace est celui du ciblage. Imaginez que vous possédez une installation nucléaire et qu'un déni de service soit lancé contre votre réseau d'électricité. Des paquets de données arrivent du monde entier et vous décidez de riposter de la même façon.

La technique des cybercriminels consiste actuellement à prendre le contrôle de milliers d'appareils grand public à l'aide de « botnets » (réseaux de machines piratés connectées à l'Internet), à les diriger vers la cible et à faire un tir groupé de paquets. Si vous ripostez, vous allez éliminer beaucoup d'appareils appartenant à des particuliers, mais pas la personne qui vous attaque. Cette personne remontera un nouveau « botnet » et recommencera. Comme je l'ai dit, il est très difficile d'identifier la source, il est très difficile de savoir sur qui tirer.

J'ajoute que l'on parle de plus en plus de la cyberguerreMais en même temps je constate à travers mes lectures que de plus en plus de personnes contestent la notion même de cyberguerre. Il est vrai que lorsqu'on étudie l'histoire de la guerre, on constate que les pays qui s'y engagent, si ce n'est pas pour se défendre, c'est pour acquérir des territoires ou des avantages politiques. Or il est très peu probable, du moins à notre époque, qu'en envoyant de simples paquets de données par l'Internet il soit possible de renverser un régime, de mettre la main sur des ressources minérales ou toute autre action de ce genre. Il y a un courant de pensée qui progresse en ce moment et qui croit qu'une cyberattaque, dans un contexte de guerre cybernétique, sera effectuée plutôt en liaison avec une action physique que de manière autonome.

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

Il nous faudra mener la réflexion bien plus loin avant d'en arriver à un OTAN cybernétique. Pour finir, je souhaite aborder un dernier sujet, Monsieur Amano, avant que nous passions aux questions/réponses. Ce sujet avait été un des fils conducteurs de la table-ronde précédente : il s'agit de l'Iran. En 2011, votre agence (l'AIEA) a rendu compte avec une remarquable franchise de l'effort continu que fournit l'Iran pour militariser son programme nucléaire. Comment se fait-il que vous ayez pu publier ce document ? Et qu'est-ce qui explique la différence de ton entre ce rapport et les précédents ?

Yukiya AMANO, Directeur général de l'AIEA

Cette question nucléaire iranienne a une longue histoire, et elle est très complexe. En résumé, l'Iran a ratifié le Traité sur la non-prolifération des armes nucléaires et a signé avec l'AIEA un accord global relatif à l'application de garanties de sécurité qui a instauré le système de vérification que l'AIEA applique à l'Iran. Nous sommes donc en mesure de vérifier que les matières et les installations nucléaires officiellement déclarées par l'Iran sont utilisées à des fins pacifiques. En revanche, la situation est comparable à la lune en quartier : la moitié des activités est en pleine lumière et il y a la face sombre. Nous ne savons pas, nous ne savons pas exactement ce qu'ils font en cachette. Certaines informations indiquent que l'Iran s'est engagé dans des activités qui correspondent au développement de dispositifs explosifs nucléaires,.

Les informations qui vont dans ce sens se faisant de plus en plus nombreuses, nous devons les vérifier par recoupement, pas une fois, mais deux fois, trois fois. N'ayant pas accès aux installations, nous ne pouvons pas l'affirmer à 100%. Cependant, nous avons des doutes sérieux. J'ai donc jugé qu'il était temps que nous alertions le monde. L'objectif de l'AIEA n'est pas de rendre un verdict de culpabilité. Notre objectif est d'empêcher la prolifération des armes nucléaires. Si certaines informations ont indiqué qu'il y avait des risques de ce côté, j'ai pensé qu'il était préférable de les diffuser pour alerter le monde.

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

Combien de temps leur faudra-t-il pour arriver à fabriquer la bombe ?

Yukiya AMANO, Directeur général de l'AIEA

C'est difficile à dire. Nous n'avons pas vocation à faire de la prospective militaire.

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

Je comprends.

Michael ANCRAM, ancien chef adjoint du parti conservateur, Royaume-Uni

Mon nom est Michael Ancram, du Royaume-Uni. J'ai deux questions, dont la première me semble plutôt être un commentaire. Chaque fois que quelqu'un nous parle du problème de la sécurité nucléaire, il a une tendance certaine à essayer de rassurer les gens en leur disant que la situation n'est pas aussi grave que on le pense. Je suis originaire d'Ecosse, et 26 ans après le désastre nucléaire de Tchernobyl, qui s'est passé à 1,000 miles de distance, il y a encore des terres agricoles où il est interdit d'élever du bétail. C'est parce que ces terres sont encore contaminées par du césium, qui n'est pas arrivé directement de la centrale, mais a été apporté par les nuages de pluie sur une longue période de temps. Si un tel accident se reproduisait, comment serions nous assurés de pouvoir contrôler la quantité des radiations dispersées sur une large zone par les conditions météorologiques ?

La deuxième question est un peu plus technique. L'attaque informatique dont l'Iran a fait l'objet, quoique nous n'en connaissions pas la source, a été exécutée par un ver (programme autoreproducteur) appelé Stuxnet. J'ai cru comprendre qu'un ver est différent d'un virus et qu'il est beaucoup plus facile à créer. Il peut être introduit dans une machine, puis, au fil du temps, il peut progresser jusqu'à la machine cible que son programme lui avait assignée. Une fois qu'il est en place, il peut rester en sommeil pendant des mois ou même des années, si nécessaire, jusqu'au moment où il doit être déclenché. Vous ne savez pas qu'il est là car il est quasi impossible de le détecter. Selon vous, combien de vers de ce type ont été créés et introduits au cours de ces deux dernières années ?

Yukiya AMANO, Directeur général de l'AIEA

D'abord, pour répondre à votre première question, il serait inexact de dire que les centrales nucléaires sont sures à 100%. Des accidents sont toujours possibles. Pour les prévenir, il nous faut développer de multiples moyens de protection. Cette fois-ci, l'accident a été provoqué par un tsunami dont l'ampleur a largement dépassé toutes les prévisions. Il y a diverses façons de protéger les réacteurs de catastrophes naturelles majeures de cet ordre. Actuellement, après Fukushima Daiichi, nous prenons des mesures pour essayer d'améliorer la sécurité des centrales nucléaires. Les centrales de la génération actuelle sont beaucoup plus sûres que les précédentes. Dans les réacteurs du futur, dits « de 4^{e} génération », les dispositifs de sécurité seront les éléments les plus importants.

Par ailleurs, nous développons une culture de la sécurité, en renforçant les organismes de réglementation, en formant les gens à opérer de façon plus efficace, et en améliorant la conception et la construction. Dans ces conditions, je pense qu'il est possible de réduire au minimum le risque d'accidents. Les leçons apprises de Tchernobyl ont été très utiles lors de l'accident de Fukushima Daiichi. Grâce à elles, le gouvernement japonais a fait évacuer les gens pour qu'ils ne soient pas exposés aux radiations. L'AIEA a envoyé une mission pour décontaminer le sol. Il existe en réalité plus de 60 technologies pour décontaminer le terrain et les installations. Même si, comme je l'ai déjà dit, il n'est pas possible de garantir une sécurité à 100 %, nous avons les moyens de réduire le risque à un minimum dans le cas où ce désastre se reproduirait.

En ce qui concerne Stuxnet, nous avons en effet visité les installations d'enrichissement de Natanz en Iran. Cependant, notre objectif n'est pas d'étudier à quel point Stuxnet est ou non efficace , mais de nous assurer que les matières et les installations nucléaires ne sont pas détournées à des fins militaires, mais utilisées uniquement dans le domaine civil. Notre connaissance des effets de Stuxnet reste donc très limitée.

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

Scott, pourriez-vous donner votre avis ? Quel est votre point de vue de professionnel sur Stuxnet ?

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

À ce sujet, je dirais deux choses. D'abord, pour ce qui est du nombre de logiciels latents existant dans le monde, si je vous disais un chiffre, ce serait pure spéculation. Ceci étant dit, j'indiquerai deux points dont il faut avoir bien conscience. Le premier est que malgré toute sa furtivité et son camouflage, Stuxnet a été détecté, comme tant d'autres logiciels malveillants. Rappelez-vous que quand un ver pénètre dans un réseau, il est souvent localisé par les systèmes de détection d'intrusion, de contrôle des sorties et par d'autres outils informatiques.

Deuxièmement, il est techniquement difficile de déployer un code pour logiciel dormant. Rien n'est impossible, bien sûr, mais le problème est que les systèmes évoluent constamment. Si les machines sont remplacées, c'est raté. Si les systèmes d'exploitation sont mis à jour, les applications sont corrigées. Par conséquent, si vous projetez d'implanter un code qui puisse être déclenché 3 à 5 ans plus tard, les chances qu'il reste intact pendant tout ce temps dépendent du système visé.

Il existe des systèmes longue durée, tels que les distributeurs automatiques de billets qui sont conçus pour fonctionner pendant 20 à 25 ans. Au contraire, les ordinateurs personnels et les serveurs, par exemple, qui font fonctionner des systèmes, ont une durée de vie beaucoup plus courte. En général, ils sont considérés comme obsolètes et remplacés dans les 3 à 5 ans, ce qui représente un environnement difficile, tant en matière d'attaque qu'en matière de défense.

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

D'après ce que vous avez lu sur Stuxnet, ce virus possède-t-il des caractéristiques qui permettraient d'avoir une idée de sa provenance ?

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

Une analyse publique a été faite à ce sujet, mais, pour être franc, elle s'est plus centrée sur l'identification de la cible et des motifs probables de l'attaque que sur l'attribution de l'auteur ou de la source du code. Au fil des années, des chercheurs ont essayé de mettre en évidence une « signature » des logiciels malveillants. De même qu'un écrivain ou un peintre a son style propre, les programmeurs ont leur propre style. On a essayé, épisodiquement, de caractériser ces styles. Malheureusement, à la différence d'une rédaction, qui permet d'écrire dans un langage fleuri ou au contraire très factuel, tout code a une syntaxe fixe. Il doit être élaboré selon certaines règles, faute de quoi il ne pourra ni se constituer ni s'exécuter. Cependant, comme je l'ai dit, des chercheurs continuent encore maintenant à rechercher des spécificités dans l'écriture de codes, pour essayer d'en identifier la source.

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

Je suis sûr qu'il y a un Ernest Hemingway parmi les programmeurs quelque part dans le monde !

Jean de KERVASDOUE, Professeur de santé publique, CNAM

Bonjour, je suis Jean de Kervasdoué, professeur de santé publique. À la suite de toutes ces interventions, il me semble que nous devrions nous pencher sur la définition de ce qu'est une catastrophe. Je suis étonné que personne n'ait évoqué le fait que le plus grand désastre de ces deux dernières années n'est pas du tout Fukushima, mais l'inondation au Pakistan qui, comme vous le savez, a submergé une zone d'une superficie supérieure à l'Autriche. Vingt millions de personnes ont été déplacées et 10,000 ont péri. Nous parlons de l'énergie nucléaire avec une crainte bien fondée et je pourrais y revenir, en analysant les conséquences de Tchernobyl. Cependant, nous ne parlons pas de la pollution atmosphérique en Chine : 400,000 personnes sont en train d'en mourir actuellement. Le danger que représente l'extraction houillère sur une année est bien supérieur à celui de toute l'industrie nucléaire civile depuis qu'elle a commencé à exister.

Comme vous le savez, l'Organisation Mondiale de la Santé (OMS) a fait un rapport sur les décès à Tchernobyl. Le nombre de victimes décédées qui ont pu être décomptées est de 56, celui des personnes qui pourraient décéder ou avoir une espérance de vie diminuée suite à l'accident est de 14,000 à 16,000 sur 50 ans. Il s'agit des estimations de l'OMS. Vous pouvez le vérifier. L'industrie houillère tue 20,000 personnes par an. Alors, qu'est-ce qu'une catastrophe ? Je pense que nous devrions revoir notre définition du terme « catastrophe. »

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

J'apprécie les ajouts que vous avez apportés à notre liste de catastrophes et je pense que votre remarque est juste. Ce que nous essayons de faire ici, c'est de traiter deux sujets qui préoccupent particulièrement les gens.Peut-être préoccupent-ils également les médias. J'accepte votre remarque et la critique qu'elle sous-entend.

Stewart PATRICK, Senior fellow et directeur du programme sur les institutions internationales et la gouvernance mondiale, Council on Foreign Relations (CFR)

Bonjour, je suis Stewart Patrick, du « Council on Foreign Relations ». J'ai deux questions, dont la première s'adresse à monsieur Amano. Vous avez mentionné la crainte que l'Iran, par exemple, pourrait détourner une partie de son matériel nucléaire au profit d'un programme d'armement. Je souhaiterais savoir où en sont les discussions sur la création d'une banque internationale du combustible nucléaire, qui pourrait aider à résoudre certains de ces problèmes ?

Je souhaiterais ensuite interroger Monsieur Charney. Vous avez mentionné un certain nombre d'avantages que nous a procuré le cyberespace. Vous avez dit que l'Internet est régi de manière assez libre par des sociétés privées et vous avez parlé du rôle joué par l'ICANN, entre autres. Cependant, je me demande si nous ne sommes pas sur la voie d'une confrontation majeure avec certains gouvernements. Ceux qui bien souvent respectent des valeurs différentes. Dans une séance précédente, Thierry de Montbrial a évoqué la diversité croissante qui caractérise le monde actuel.

Vous avez analysé plusieurs types de risques en matière de sécurité de l'Internet ou du cyberespace. Il y a la cybercriminalité, évidemment, contre laquelle beaucoup de gouvernements s'unissent. Il y a aussi le cyberespionnage et la cyberguerre. Ceci pose la question de la nécessité d'établir un traité définissant les utilisations

potentielles et les utilisations légitimes du cyberespace, sur le modèle des droits de la guerre. Cependant, il existe une autre grande question, celle des droits de l'homme et du libre accès à l'Internet. La Secrétaire d'État Hillary Clinton dénonce les pays qui s'opposent à la vision américaine d'un Internet ouvert, privé, et en grande partie anonyme. Pourtant, ces principes sont contestés, même par certaines démocraties telles que l'Inde. Pourriez-vous nous éclairer sur ce dilemme ?

Yukiya AMANO, Directeur général de l'AIEA

Je répondrai d'abord à la question concernant la création d'une banque du combustible nucléaire, en expliquant brièvement sa nature et en précisant où nous en sommes. C'es dernières années, en particulier, nous avons observé que de plus en plus de pays ont manifesté un intérêt pour l'énergie nucléaire. Si cette tendance se poursuit, le besoin de combustible nucléaire va s'accroître en conséquence. Il est normal que ces pays qui pensent se tourner vers les centrales nucléaires s'inquiètent d'une pénurie de combustible. L'établissement de cette banque a pour but de créer une réserve qui permettra de pallier aux problèmes d'approvisionnement liés à des raisons non commerciales.

Nous avons reçu quelques propositions dans ce sens, dont une de la Russie, qui a proposé l'établissement d'une banque internationale de combustible nucléaire sur son sol. Cette proposition a été adoptée par le Conseil des Gouverneurs, l'organe de décision de l'AIEA. La décision a été prise il y a environ deux ans et de l'uranium faiblement enrichi est stocké conformément au système de garanties de l'AIEA. Cette banque du combustible nucléaire existe donc dans la réalité, et elle est opérationnelle.

Une autre idée est d'établir une banque du combustible propre à l'AIEA. Encore une fois, la décision de principe a déjà été prise et nous sommes maintenant dans la phase de réalisation. Nous avons invité des pays à héberger cette banque et l'un d'entre eux a postulé et exprimé son intention de l'héberger. Nous sommes actuellement en train de prendre les dispositions nécessaires à l'approvisionnement en uranium faiblement enrichi, et nous nous préparons à conclure cet accord ainsi que quelques autres points. Nous disposons déjà des fonds nécessaires à l'achat de l'uranium enrichi. Le Royaume-Uni a proposé un autre projet visant à garantir l'achat d'uranium enrichi. En l'état actuel, nous disposons donc d'une banque internationale du combustible et d'un système de garantie, et un autre système de réserve, propre à l'AIEA, est en cours de préparation.

Scott CHARNEY, Vice-président de Trustworthy Computing, Microsoft

Revenons à vos questions. Vous avez parlé de cybercriminalité, de cyberespionnage, de cyberguerre et de liberté d'expression. Tout cela montre à quel point l'Internet transforme désormais tout ce que nous faisons. Dans le passé, des pays comme la Russie ont proposé avec insistance une sorte de traité sur la guerre cybernétique, tandis que d'autres pays se sont montrés réticents, en partie à cause de l'impossibilité de vérifier l'application de ce genre de traité.

Cela dit, des discussions sont menées actuellement sur la nécessité ou non d'une Convention de Genève pour l'Internet. Un point très important est la différence de terrain : dans la guerre traditionnelle, le champ de bataille est naturel alors que sur l'Internet il est artificiel. En général, la victoire exige l'utilisation de canaux de communication dont la plupart sont entre les mains du secteur privé. Dans certains pays, les télécommunications sont encore nationalisées, ce qui implique une sortie secteur privé.

Le défi posé aux pays, au secteur privé comme aux citoyens, réside dans le fait que l'Internet est un partagé et intégré. En effet, il est accessible aux particuliers, aux entreprises et au gouvernement via des activités dont la variété est fonction de la liberté d'expression, y compris l'envoi de paquets d'espionnage et, potentiellement, de paquets de guerre. Ces éléments sont intégrés de telle sorte qu'ils ne peuvent pas être traités séparément. Autrefois, en temps de guerre, vous pouviez faire voler un ballon anti-aérien ou afficher une grande Croix-Rouge sur le toit d'un bâtiment

pour montrer qu'il s'agit d'un espace protégée. Il était interdit de lancer une bombe sur cet espace à cause des risques de dommages disproportionnés aux civils. Sur l'Internet, la difficulté vient du fait que tout se ressemble : tout n'est qu'adresses IP. Même si certaines personnes ont commencé à travailler sur des lois des conflits armés et une Convention de Genève relative au cyberespace, cette législation est difficile à appliquer.

En matière de liberté d'expression, rappelons que Microsoft participe au Global Network Initiative (l'Initiative mondiale des Réseaux TIC) qui regroupe des sociétés et des organisations non gouvernementales engagées dans la protection des libertés d'expression et d'association sur Internet. La difficulté est que cette liberté d'expression n'est pas un lieu, mais un continuum, dont une extrémité est constituée par les États-Unis et son Premier Amendement, ce qui signifie en pratique l'élimination de toute limitation préalable à la liberté d'expression. A l'autre extrémité se trouvent des pays, y compris des pays démocratiques, qui réglementent beaucoup plus la liberté d'expression. L'Allemagne, le Canada et le Royaume-Uni ont des lois sur les discours haineux, sur la propagande néo-nazie etc. Enfin, il y a des régimes répressifs.

En dernière analyse, tout ce que nous venons de voir a trait aux différences culturelles quant à la liberté d'expression, mais aussi à la forme de gouvernement et au pouvoir de décision. Comme vous pouvez l'imaginer, c'est un terrain assez litigieux. Lorsque j'ai présidé le sous-groupe du G8 sur la criminalité liée aux technologies de pointe, le G8 était en train d'élaborer un ensemble de principes pour la cybercriminalité. Voici comment les choses se passaient : pour commencer, nous nous mettions d'accord sur tout ce qu'il fallait faire pour combattre la cybercriminalité. Ensuite, les délégations des autres pays disaient ceci à la délégation des États-Unis : « Nous allons maintenant aborder la question des restrictions à la liberté d'expression. Vous devriez quitter la pièce pour faire une pause-café. » Puis, en notre absence, ces pays rédigeaient un protocole d'accord et une note additionnelle. Toutes les délégations signaient l'accord, mais seule la délégation des États-Unis refusait de signer la note additionnelle parce que les restrictions à la liberté d'expression violaient la constitution américaine.

J'ajouterai encore une chose qui m'a toujours stupéfié. Très souvent, on aborde un problème sous un certain angle sans penser à d'autres manières de voir. Dans le cadre de l'Initiative mondiale des Réseaux TIC, beaucoup de monde s'inquiète de la liberté d'expression en général et sur l'Internet, en récusant la censure ou les restrictions à la liberté d'expression. Il n'empêche que pendant le Printemps Arabe, le gouvernement égyptien a ordonné à Vodafone d'envoyer un message qui ressemblait à de la propagande. L'entreprise aurait perdu sa licence si elle avait refusé. Elle a donc envoyé le message tout en jouant la transparence en déclarant : « nous avons diffusé ce message à la demande du gouvernement. » Autrement dit, il ne s'agit pas seulement d'un problème de restriction à la liberté d'expression, mais aussi d'un problème de discours contraint, qui est différent, mais tout aussi grave.

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

Je pense que cette discussion a été très enrichissante; et que c'est un excellent mot de la fin. Si nous pouvions établir une banque de combustible nucléaire vraiment crédible, je ne peux imaginer meilleure contribution à la gouvernance mondiale. Je tiens à remercier nos intervenants pour l'excellent programme de ce soir. Et je veux remercier l'assistance pour être restée jusqu'à la fin.