MEIR SHEETRIT

Membre de la Knesset, ancien ministre responsable des services de renseignement, Israël

Bonjour à tous. Je suis très heureux d'être ici. C'est merveilleux d'être de nouveau à vos côtés dans ce panel. On vous a présenté certains des avantages d'Internet. La Toile rend nos vies plus faciles et plus confortables. Elle nous permet un meilleur accès. J'aimerais maintenant évoquer certains inconvénients qu'elle présente. Le champ de bataille moderne a changé radicalement. Il n'est plus seulement question d'avions, de tanks ou d'infanterie. La cyberguerre fait désormais partie de l'équation. Depuis le milieu des années 1990, on observe ce type de guerre. Les deux objectifs des cyberguerriers sont premièrement, de paralyser les sites et d'y laisser une signature afin de vous montrer qu'ils sont passés par là, que vous êtes vulnérable et qu'ils peuvent revenir à tout moment et faire ce qu'ils veulent, et deuxièmement, d'endommager les infrastructures.

Au cours de la deuxième guerre du Liban entre Israël et le Hezbollah, nombre de hackers ont lancé de grosses attaques contre les sites israéliens. En réaction, nombre de hackers israéliens ont attaqué les sites du Hezbollah. Nous avons observé en temps réel les dégâts générés des deux côtés. De nos jours, pour faire s'effondrer un régime, on n'a plus besoin de le conquérir ni de l'attaquer physiquement avec son armée. On n'a plus besoin de tanks, ni d'avions. Tout ce qu'il faut, c'est un ordinateur et un clavier. Nous ne sommes pas loin de cette éventualité. À l'été 2007, l'Estonie a été attaquée par des hackers, probablement des Russes, et l'État s'est effondré. Les infrastructures se sont effondrées. Les communications ont cessé de fonctionner. Les banques et l'électricité ont été coupées. Et ce n'était qu'une démonstration de ce qui peut être réalisé. La cyberguerre peut paralyser un État entier.

De nos jours, l'un des objectifs des hackers est de prendre ce type de contrôle sur les États de façon à gagner de l'argent par chantage. Ils peuvent la menacer de paralyser un pays s'ils n'obtiennent pas un paiement. Être dans cette position assurerait un réel pouvoir, et ce n'est pas impossible. L'un des objectifs de ces hackers est de disposer d'un contrôle suffisant sur les États pour pouvoir leur extorquer de l'argent.

J'aimerais vous faire part de quelques expériences israéliennes en matière de cyberguerre et de notre manière d'appréhender cette question. Vous le savez, nous vivons dans un voisinage très difficile. Je tiens à informer de ces expériences parce que je pense que vous avez besoin d'en tenir compte dans vos pays respectifs. Il y a quelques années, nous avons mis en place l'INCB, l'Israeli National Cyber Bureau. Il n'a été formellement instauré par le gouvernement qu'en 2012, mais en réalité nous avons commencé à le mettre en place il y a cinq ou six ans. Ce bureau intègre nombre d'organisations et d'unités du ministère de la Défense et des services de sécurité. Tous sont placés sous l'autorité du Premier ministre. Je vais tâcher de vous expliquer pourquoi.

Il ne s'agit pas uniquement d'une question de défense et de sécurité car, dans ce cas, toutes ces unités seraient placées sous la responsabilité du ministère de la Défense. Je l'ai dit, beaucoup de dégâts peuvent être générés par le biais de votre infrastructure. Vous devez par conséquent la protéger. Pour ce faire avec succès, il ne suffit pas d'avoir quelques personnes chargées de cette mission. Vous devez couvrir un très vaste système, ce qui signifie que vous avez toujours besoin de préparer vos combattants à protéger votre Internet, vos sites et votre infrastructure. Vous devez en permanence développer de nouvelles technologies, et par conséquent mener des recherches. Pour disposer des recherches adéquates, vous avez besoin de nombreux étudiants qui étudient la physique et les mathématiques à un très haut niveau. Vous devez veiller sur les nombreux systèmes de votre pays afin de disposer des capacités de défense et d'attaque si vous en avez besoin. C'est pour cette raison que nous plaçons ce bureau sous l'autorité du Premier ministre, car il faut quelqu'un qui dispose de suffisamment de pouvoir pour piloter tous ces systèmes.

Quelles en sont les principales caractéristiques ? Je l'ai dit, l'une d'entre elles porte sur la protection des systèmes informatiques du gouvernement. Chaque gouvernement dispose de sites e-gouvernementaux qui permettent aux populations d'accéder à divers services publics. Une attaque de ces sites peut paralyser le fonctionnement des services gouvernementaux, dont les populations dépendent. Deuxième caractéristique, la protection de l'infrastructure principale. De nos jours, la plupart des éléments d'infrastructure sont contrôlés par des ordinateurs et si vous

réussissez à accéder à ces ordinateurs, vous pouvez faire ce que vous voulez à l'intérieur des systèmes. Par exemple, vous pourriez prendre le contrôle du système des feux de signalisation d'un pays et le modifier comme bon vous semble. Les faire tous passer au vert, par exemple. Ce serait une catastrophe et c'est pourtant une chose très simple. Vous pourriez également paralyser la production d'électricité d'un pays si vous accédez aux ordinateurs qui contrôlent les centrales électriques du pays. Il en va de même pour les centrales nucléaires. Si vous avez accès aux ordinateurs qui les contrôlent, vous pouvez faire beaucoup de dégats.

Protéger les infrastructures est essentiel pour les États s'ils veulent maintenir leurs systèmes opérationnels. C'est pour cette raison que nous avons établi tant d'unités avec cet objectif. Il y a une unité au ministère de la Sécurité publique, en charge de la protection de l'infrastructure principale connectée et contrôlée par des ordinateurs. Des unités spéciales protègent également nos sites e-gouvernementaux contre d'éventuelles attaques.

À l'évidence, vous avez entendu parler du ver Stuxnet qui a attaqué les centrifugeuses iraniennes. C'était un virus très complexe qui a provoqué énormément de dégâts. Les Iraniens ont mis deux ans à l'identifier. Quand un virus est utilisé de manière offensive, comme c'est le cas ici, la question se pose de savoir comment les hackers empêchent ce virus de contaminer leur propre système. Dans le cas de Stuxnet, par exemple, le virus était tellement sophistiqué qu'il n'était actif que dans certains types de centrifugeuses, utilisées uniquement en Iran. Il ne fonctionnait pas s'il infiltrait d'autres types de centrifugeuses dans d'autres pays. Quand les Iraniens l'ont identifié, ils l'ont envoyé à un laboratoire en Russie. Les Russes ont enquêté et révélé au monde l'existence de ce virus.

Je cite cet exemple parce qu'il n'y a pas d'ordinateurs dans les centrifugeuses. Il s'agit juste de machines mécaniques équipées de moteurs électriques qui les font tourner très très vite. Elles sont en revanche supervisées par des ordinateurs. Si vous pouvez infiltrer ces ordinateurs, alors vous pouvez provoquer des dommages considérables aux centrifugeuses. C'est ce qui s'est passé en Iran.

Quelles sont maintenant les principales caractéristiques de la cyberguerre ? Attaquer les principaux éléments de l'infrastructure d'un pays comme son alimentation en eau, en électricité, son système de transport, ses banques, ses marchés boursiers, sa communication, etc. Vous pouvez réellement attaquer tout ce que vous voulez et paralyser tout un pays. Stuxnet constitue un bon exemple de cyberattaque. Souvenons-nous de l'attaque de 2007 sur l'Estonie. En juin 2010, Stuxnet était à l'œuvre en Iran. En mars 2011, la NASA a admis qu'en deux ans 13 attaques réussies avaient été lancées contre ses systèmes informatiques et qu'elle avait perdu le contrôle de la station spatiale.

Le 28 mai 2011, Lockheed Martin a découvert que ses nouveaux systèmes informatiques venaient de subir une très violente attaque. Les agresseurs avaient dérobé tous les plans des nouveaux avions de Lockheed Martin, comme les F-35, qui sont des armes stratégiques très sophistiquées. Tout avait été dérobé. On a soupçonné la Chine d'être à la manœuvre. Pourquoi ? Habituellement les gens n'attaquent pas les sites depuis leur propre pays. Ils transitent en général par un serveur situé dans un pays différent et éloigné afin qu'il ne soit pas possible de leur attribuer l'attaque. Selon les Américains, Lockheed Martin est si bien protégé qu'une attaque réussie requiert des centaines de personnes travaillant à cet objectif pendant au moins quatre ans, et seule la Chine est à même d'organiser une opération de cette envergure.

En septembre 2011, des hackers iraniens ont pénétré les ordinateurs d'une société de sécurité informatique des Pays-Bas et falsifié des documents qui leur permettaient d'accéder aux sites du Mossad, de la CIA et du MI6. En décembre 2011, des hackers saoudiens ont annoncé avoir téléchargé les informations de cartes de crédit de 400 000 israéliens. En réaction, les hackers israéliens ont pénétré les données des cartes de crédit saoudiennes. Ce fut une grosse bataille à l'époque. En novembre 2011, des hackers ont pris le contrôle des systèmes de pompes à eau dans les États de l'Illinois et du Texas. Sans provoquer de dégâts. Ils voulaient juste montrer aux États-Unis que le pays n'était pas protégé et qu'il était lui aussi exposé à ce type d'attaque. En mai 2012, le virus Flame a été dévoilé, que les experts pensent être 20 fois plus puissant que Stuxnet.

Nous avons par conséquent décidé que nous avions besoin d'un écosystème pour faire face à tous ces problèmes. Il ne s'agit pas seulement d'une question d'attaque et il ne s'agit pas seulement d'une question de défense. Vous avez besoin des deux capacités et vous en avez besoin simultanément. C'est pour cette raison que vous avez besoin d'un écosystème plutôt que de différentes stations. Les choses doivent être synchronisées. Pendant la Seconde Guerre

mondiale, les forces aériennes du Royaume-Uni étaient divisées en trois corps différents, le premier pour protéger les côtes anglaises, le deuxième pour protéger l'espace aérien et le troisième pour attaquer en dehors de l'Angleterre. C'est aujourd'hui impossible. L'armée de l'air est désormais une seule entité. De la même manière, nous avons besoin que tout ce qui a trait au cyberespace soit fortement synchronisé au sein d'un système unique afin d'empêcher certaines situations.

Pour vous donner un exemple hypothétique, nous aimerions transférer des informations depuis certains ordinateurs. Dans un même temps, d'autres cyberunités vont attaquer ces ordinateurs pour les paralyser. Cela serait stupide. Nous avons besoin que nos ordinateurs restent actifs pour pouvoir en extraire les informations. Vous avez par conséquent besoin d'une très bonne synchronisation. C'est pour cette raison que nous avons besoin d'un tel écosystème. Bien entendu, y parvenir présente des obstacles et des difficultés. Pourquoi ? Parce que vous avez besoin de régulation. Les pouvoirs publics ont besoin de formuler des législations spécifiques afin de protéger chaque infrastructure. Sinon vous ne le pouvez pas. Même si vous en avez les moyens et la capacité, vous n'en avez pas le droit.

Aux États-Unis par exemple, l'un des problèmes rencontrés par le gouvernement est qu'il refuse d'endosser la responsabilité de la protection du système financier privé car cela enfreindrait le droit à la confidentialité. Je pense que c'est une erreur car il est facile d'attaquer ces systèmes. Imaginez que vous vous rendiez dans une banque en Israël et que vous annonciez vouloir protéger leur site contre une attaque extérieure. La banque vous répondrait que, si des mesures de protection des clients sont en place, cela peut signifier que des gens consultent des comptes privés, ce qui constitue une violation des règles de confidentialité. Là encore, vous avez besoin de légiférer pour équilibrer les préoccupations liées au respect de la confidentialité et les besoins de protection. Car la confidentialité reste bien entendu très importante.

En ce qui concerne les développements technologiques, la plupart du temps, les changements demandent 10 à 20 ans. Regardez les voitures. Après que la voiture a été inventée, il a fallu de nombreuses années pour de réels changements soient apportés au design. Dans la technologie du cyberspace, une génération s'étend sur un an et demi, pas plus. Vous ne pouvez par conséquent pas demander à un expert de mettre en place un système qui protège votre pays puis l'oublier pendant les cinq à dix années à venir. Au risque sinon de vous réveiller un jour avec une catastrophe absolue. Vous devez assurer un suivi constant. Vous devez vous occuper de ces systèmes au quotidien, en développant en permanence la technologie. Au bout d'un an, un an et demi, la technologie sera déjà radicalement différente. Si vous n'êtes pas préparé, vous n'aurez plus de protection. Tout ce que vous avez fait sera caduc. Cette technologie requiert un développement constant et vous devez toujours être en alerte.

La technologie ne suffit pas. Beaucoup de choses peuvent faire des dégâts d'une façon surprenante si quelqu'un décide de vous attaquer. Disposer de la technologie ne suffit pas. Vous avez besoin des bons guerriers. Le général Alexander des États-Unis a déclaré que devenir un cyberguerrier nécessite d'avoir une dizaine d'années d'expérience dans la construction des réseaux, leur défense et dans la pratique du cyberespace. Combien de personnes ont une telle expérience ? Très peu. David Dittrich a déclaré que nous pouvons raisonnablement estimer qu'il faut plus de dix ans d'expérience au niveau le plus élevé d'opérateur réseau pour acquérir la capacité de défendre et d'attaquer dans la cyberguerre. Ce qui signifie que vous devez investir beaucoup d'argent et de temps pour éduquer ces cyberguerriers. Vous ne pouvez vous contenter d'amateurs. Vous avez besoin de professionnels qui consacrent leur vie à cette discipline.

Les États-Unis recensent environ trois millions d'informaticiens. 60 % d'entre eux vivent dans la peur car ils ne connaissent rien au cyberespace et ne sont pas capables de protéger leurs propres systèmes. Le budget des États-Unis pour le cyberespace s'élève à l'heure actuelle à 4,7 milliards de dollars US par an. Je ne connais pas les budgets de vos pays respectifs mais je vous suggère de les doubler. Vous avez besoin de beaucoup plus. Vous avez besoin d'investir beaucoup si vous souhaitez vous protéger.

Nous parlons par conséquent d'un écosystème général qui doit englober l'industrie, la sécurité, l'éducation, le gouvernement et la législation. Vous devez vous occuper de tous ces aspects et les synchroniser. Israël est une cible. Israël est la cible la plus attaquée dans le monde. Nous enregistrons près de 100 000 attaques par jour. Dans les périodes comme la guerre de Gaza ou la guerre du Liban, nous recensons plus d'un million d'attaques par jour. Cependant, le Rapport des menaces McAfee, qui évalue les pays en fonction de leur niveau de protection, classe

Israël parmi les pays les mieux préparés à une cybermenace aux côtés de la Suède et de la Pologne. Malgré le nombre de gens dans de nombreux pays qui veulent attaquer Israël, le pays bénéficie d'une protection adaptée car nous sommes préparés. Il le fallait. Je l'ai dit, nous vivons dans un environnement très difficile, aussi nous devons êtes préparés aux attaques.

Je pense que nous avons en général peur de ce que nous ne connaissons pas. Par conséquent, notre mission dans chaque pays est de nous renseigner très sérieusement sur la question et d'investir les fonds nécessaires afin de préparer les bonnes personnes à nous protéger. Nous serons sinon en très mauvaise posture si nous traversons une guerre ou un conflit. J'aimerais pour conclure rappeler qu'un jeune homme vaut parfois bien plus qu'une simple division armée. Un bon cyberguerrier peut causer plus de dégâts que n'importe quelle division armée ou n'importe quelle force de frappe aérienne. C'est incroyable, mais c'est la réalité. Merci.