MEIR SHEETRIT

Ancien membre de la Knesset, ancien ministre des Renseignements et du Comité de l'Énergie atomique, ancien ministre de l'Intérieur

Thomas GOMART

The floor is yours.

Meir SHEETRIT

Merci beaucoup. J'aimerais expliquer en termes très simples ce qui se passe dans le domaine de la cyberguerre. Comme l'a indiqué notre modérateur, il y a six ans, à Monaco, j'ai participé à une session sur le cyberespace, au cours de laquelle j'ai expliqué la menace qu'il représente. La mauvaise nouvelle c'est que la situation s'est énormément aggravée. Je vous avais dit à l'époque que tout ce que vous écriviez sur votre iPhone, vos SMS, vos appels, quoi que ce soit, où que vous soyez, tout pouvait être vu par quiconque avec un minimum d'efforts. Aujourd'hui, c'est non seulement toujours possible, mais il est même possible d'inverser la fonction d'appareil photo de votre téléphone. À partir de votre appareil photo, des photos peuvent être prises de l'endroit où vous vous trouvez et il est possible de vous écouter. Peu importe où vous êtes, en réunion, chez vous, vous pouvez être écouté, même de très loin. Thierry, j'aimerais un jour avoir l'occasion de faire venir d'Israël des spécialistes qui pourraient démontrer aux personnes ici présentes qu'ils peuvent contrôler n'importe quel téléphone dans la salle. Ils le feraient bien sûr uniquement avec des volontaires. Ils vous montreraient en cinq minutes qu'ils peuvent voir tout ce que vous faites.

Je vais essayer d'expliquer ce qui s'est passé au cours des six dernières années. Les systèmes informatiques ont fait de très grands progrès, très rapides. Ils évoluent à une vitesse réellement stupéfiante. Il existe un graphique qui montre l'évolution des ordinateurs. On l'appelle la loi de Moore. Pour faire simple, selon la loi de Moore, ou sa version simplifiée, la vitesse des processeurs ou la puissance de traitement globale des ordinateurs double tous les deux ans. Donc, depuis 1960, date à laquelle cette loi a été présentée par Moore, la puissance des ordinateurs a été multipliée par 50 milliards. C'est un fait. C'est le graphique que je viens de vous montrer. Dans une voiture moderne aujourd'hui — dans vos voitures — il y a plus de 100 puces. La puissance de calcul de mon iPhone aujourd'hui, de vos iPhones, est supérieure à la puissance de l'ordinateur du programme spatial Apollo 11. Les choses évoluent donc très, très vite.

Maintenant, que se passe-t-il dans le monde en matière d'informatique ? Dans le passé, les infrastructures n'étaient pas informatisées. En fait, nous n'y avions pas pensé. La seule façon de les endommager ou de les atteindre était l'attaque directe. Si vous vouliez détruire, disons, une centrale nucléaire, vous deviez y aller et la bombarder. Impossible de faire autrement. Il en était de même pour les réseaux électriques, les centrales électriques, les voies navigables, quoi que ce soit. Aujourd'hui, avec l'informatisation, les choses ont changé. A l'époque, dans la plupart des pays, les infrastructures n'étaient pas informatisées. 1980 a marqué le début de différents systèmes informatiques dans le monde. Les infrastructures dans la plupart des pays ont alors été informatisées. Il s'agit notamment des banques, des structures gouvernementales, des administrations, des données, des centraux téléphoniques. Aujourd'hui, presque tout est informatisé.

Cette informatisation a créé une dépendance entre les gens et les ordinateurs. Ce qui a donné des idées à certains : « Maintenant, s'il y a tant de données et tant de possibilités, pourquoi ne pas les utiliser à notre avantage ? ». C'est ainsi que la cyberguerre a commencé. C'est depuis que les centraux téléphoniques et les dossiers des administrations ont été numérisés que des personnes mal intentionnées ont commencé à travailler et à lancer des cyberoffensives.

Mais, qu'est-ce que cela représente ? La technologie dominante du siècle est l'informatique. La cyberguerre, c'est l'utilisation des ordinateurs contre la société. C'est ce que signifie cyberguerre. Des gens utilisent nos propres systèmes informatiques à notre encontre et à leur profit. Il s'agit d'extorsion, il s'agit d'attaquer d'autres endroits, d'espionner, etc. Jusqu'en 2010, seuls les services de renseignements étaient conscients de cette cyberguerre. Personne ne s'en souciait. Jusqu'en 2010, personne ne se souciait de la cyberguerre. Quelques pays, une dizaine

seulement, dont Israël, ont commencé à s'en préoccuper. C'est seulement en 1993 que l'unité de guerre informatique a été créée au sein des services de renseignement israéliens. C'est à cette date que la cyberguerre a commencé à être prise en compte.

Il faut se rappeler que, jusqu'en 1995, chaque pays développait des ordinateurs différents. Il n'y avait pas de standardisation des ordinateurs. Ce n'est qu'en 1995 que cette standardisation a commencé. Cette absence de standardisation créait beaucoup de problèmes. Vous deviez apprendre le fonctionnement de chaque ordinateur, la manière dont il avait été construit, la façon de le connecter, etc. Avec la standardisation, la vie est devenue beaucoup plus simple pour tout le monde.

Ce n'est qu'en 2002 que l'ISA, l'Autorité de sécurité israélienne, a créé la NIS, la *National Infrastructures Security* (Sécurité des Infrastructures Nationales). La NIS a pour but d'empêcher toute attaque contre les infrastructures israéliennes par qui que ce soit, ou quelque pays que ce soit. Mais écoutez bien ceci : aujourd'hui, un bon informaticien de 20/22 ans est beaucoup plus puissant que toute une armée. Vous n'avez pas besoin de chars, d'avions ou de missiles pour semer le chaos et la destruction dans un pays. Vous pouvez le faire à partir de votre clavier, de chez vous, si vous en avez les capacités. Les choses ont changé dans le monde en ce qui concerne la façon de traiter les problèmes ou les attaques. Parce qu'Israël a quelque chose comme 100 000 attaques par jour en temps normal (en temps de guerre, les attaques sont de l'ordre d'un million par jour), nous devons être parmi les meilleurs. Sinon, nous ne pouvons pas survivre. Nous devons donc développer très, très fortement notre cyberpuissance.

En 2010, le ver Stuxnet a été découvert sur de nombreux ordinateurs dans le monde. Vous vous en souvenez ? Le monde en a été bouleversé. Pourquoi ? Parce que soudainement quelqu'un, de très loin, a ruiné toutes les centrifugeuses de l'Iran, l'empêchant ainsi d'enrichir de l'uranium. Cette attaque a été lancée à distance. Personne n'y est allé. Personne n'y a touché. Personne n'a attaqué et pourtant ils ont réussi à ruiner toute l'infrastructure iranienne de production d'uranium enrichi. Bon je ne vais pas dire qui l'a fait... c'était les États-Unis. Il y a eu des dommages matériels, mais rien n'a été volé. Ce qui a démontré au monde entier qu'il était possible d'agir de loin.

Israël a donc décidé de créer un écosystème capable de faire face à tous ces « cyberproblèmes ». Nous avons déployé de très gros efforts pour y parvenir. Des budgets ont été attribués à la recherche dans les universités, dans l'industrie. Des heures d'enseignement sur ce sujet ont été dispensées dans les lycées. Il a fallu assurer le soutien de tout le système, le gérer, le synchroniser afin que chacun sache ce que les autres font. Et ce système fonctionne vraiment très bien. Je dois maintenant vous fournir quelques données sur ce qui se passe en Israël. Ce sont des données très, très intéressantes. Par exemple, les exportations israéliennes de biens et de services ayant trait au cyberespace dans le domaine civil ont atteint 7 milliards de dollars cette année, soit 8 % du marché mondial. Or Israël ne représente que 0,1 % de la population mondiale. Les investissements mondiaux dans le secteur des cyberentreprises sont très importants. Sur le total de ces investissements, par exemple des fonds de capital-risque dédiés aux centres de développement, etc. 18 % reviennent à Israël, car Israël figure parmi les centres de développement les plus avancés dans le domaine du cyberespace. Entre 2012 et 2018, la croissance des cyberproduits en Israël a été de 600 %. Nous n'étions pas les premiers au monde, mais parmi les premiers. En revanche, nous avons été les premiers à démontrer au monde entier l'importance de ce domaine.

Je voudrais aborder deux autres points. L'affaire Snowden tout d'abord. L'affaire Snowden a éclaté en 2014/2015. Cette affaire a automatiquement créé une très forte tension entre le besoin de sécurité et la protection de la vie privée. Snowden a en effet révélé que les États-Unis suivaient chacun de nous, lisaient tous les e-mails, etc. qu'ils connaissaient ces informations. Cette affaire a créé de la méfiance vis-à-vis des gouvernements. Pour régler ce problème, en Israël, nous avons proposé et établi une unité distincte fondée sur trois principes. Premier principe : dans un pays moderne, les services de renseignement ne traquent pas les civils. Deuxième principe : création d'un nouvel organisme civil qui n'appartient pas au renseignement parce que des sociétés civiles sont nécessaires. Troisième principe : cet organisme n'appartiendra pas aux forces de l'ordre.

Si vous voulez vraiment protéger les habitants de votre pays des attaques extérieures, comment vous y prenez-vous ? Même si vous créez un organisme de ce type, vous ne pourrez pas lire tous les e-mails. Aujourd'hui, nous ne pouvons pas le faire. Dans le futur, nous ne pourrons toujours pas lire tous les e-mails, mais nous pourrons utiliser l'intelligence

artificielle, l'IA, et l'apprentissage automatique. Je vais juste vous décrire tout ceci de manière très générale. Supposons qu'il existe une machine qui lise tout ce qui se passe sur Internet en Israël, tout, très rapidement, immédiatement, dans un système très, très rapide. Cette machine fait ensuite ressortir tous les e-mails qui comportent des éléments considérés comme suspects. Ces e-mails sont transférés aux instances de surveillance pour détection. Sinon, vous ne savez pas ce qui se passe. Donc cela pourrait être fait et c'est exactement mon dernier point, à savoir le futur : la capacité à protéger le réseau ne pourra être obtenue que par l'intelligence artificielle et l'apprentissage automatique.

Dans ce domaine, il y a actuellement beaucoup de concurrence dans le monde. Les pays investissent des milliards, des centaines de milliards de dollars, pour développer ce que nous appelons les ordinateurs quantiques. Je ne m'étendrai pas sur ce sujet, mais je vais juste vous donner un exemple. Google a récemment indiqué que ses ingénieurs avaient réussi avec un ordinateur quantique de 53 qubits à réaliser un calcul en 200 secondes, calcul dont l'exécution prendrait 10 000 ans au plus gros ordinateur du monde, à la NASA. Pourquoi 200 secondes ? Parce que c'est pour l'instant la durée pendant laquelle ils parviennent à faire fonctionner un ordinateur quantique. Mais ils réussiront à créer un ordinateur quantique capable de durer, ce n'est qu'une question de temps. À partir de là, tout sera possible, car, dans le monde, tout changera, y compris votre vie. Merci.

Thomas GOMART

Thank you, Meir.