LUC-FRANÇOIS SALVADOR

PDG de Sogeti

Vos Excellences, Messieurs les Ministres,
Honorables Invités,
Mesdames et Messieurs,

Notre monde moderne est plus que jamais interconnecté. Jamais encore il n'aura été aussi facile qu'aujourd'hui d'échanger des messages électroniques, d'effectuer des virements bancaires, des commandes en ligne ou d'acheter des billets d'avion en quelques clics, à partir de son téléphone portable.

- Environ 50 milliards d'appareils électroniques seront connectés d'ici 2020, et la plupart seront mal protégés, ce qui veut dire qu'ils seront la proie de pirates qui risquent de s'infiltrer dans nos systèmes, dans nos entreprises, dans nos foyers et dans nos vies privées.

Les technologies de l'information sont au cœur de nos civilisations et de nos entreprises.

– L'accroissement du **réseautage** et des connections permet à nos entreprises d'être plus efficaces, plus productives et mieux informées.

– **L'accès aux données et à l'information** sont des atouts majeurs pour toute personne, pour toute entreprise, et pour tout pays. Les technologies de l'information sont donc devenues essentielles à la **prise de décision**.

– Elles permettent de mettre en place des **processus d'optimisation et d'industrialisation** tels que l'aiguillage ferroviaire, le contrôle du trafic aérien, la distribution d'essence et d'électricité et les réserves d'eau chlorée.

Mais **l'utilisation croissante de la technologie va de pair avec un manque de compréhension des enjeux qui en découlent**, en particulier parmi les jeunes générations : « *Cela nous est égal de savoir comment ça marche, du moment que ça marche*. »

Nous devenons vulnérables, nous sommes des cibles faciles. Nos atouts sont à la fois aussi nos faiblesses.

Au début, le **piratage** était considéré comme **un jeu**, un loisir pour une minorité de gens. Puis il est devenu un **outil idéologique et politique**, comme pour les *Anonymous*, par exemple, qui influence l'opinion publique et manipule les foules ; nous en avons eu la preuve lors du *Printemps arabe.* Mais aussi puissants soient-ils, leur objectif est pour le moment inoffensif. Bien entendu, on peut toujours dire que ce sont des « *haktivistes* », des pirates organisant davantage la **désobéissance civile** que des actions directes ou radicales. Mais pour ce qui est de publier des informations confidentielles, ils pourraient faire beaucoup de mal, et même menacer des vies humaines (voir la fuite d'informations diplomatiques publiées sur *Wikileaks,* qui mit en danger des membres du gouvernement américain lors de l'affaire du **Cablegate** en 2010-2011). Ce qui est plus perturbant encore, ce sont les millions d'utilisations criminelles de réseaux et de technologies au quotidien. Le **cyber-espionnage** est devenu courant et ce n'est qu'une question de temps avant que le **cyber-terrorisme** ne fasse son apparition.

Les frontières entre toutes ces activités sont brouillées, en grande partie du fait de la topologie de l'espace cybernétique. En dépit des règlementations, il reste une **zone d'ombre** dans laquelle des personnes bien organisées peuvent agir en toute impunité : les pirates et les espions l'ont bien compris. L'espace informatique leur fournit une parfaite couverture. La complexité du piratage le rend encore plus difficile à cerner : pas de drapeaux, pas d'uniformes, vos amis se déguisent en ennemis et vos ennemis se déguisent en amis.

Mais qu'est-ce qui rend le piratage informatique si difficilement évitable ?

- D'abord, nous n'avons à notre disposition **aucun indice** concluant, ni **aucun avertissement**. Les pirates profitent de l'effet de surprise qui aggrave la peur de l'inconnu.

- Il y a aussi une **incertitude liée au temps**, en particulier dans les activités d'espionnage. Un cheval de Troie ou un ver peut rester inactif pendant des mois avant d'être détecté, et il est donc difficile d'évaluer le volume d'information dérobé à un système informatique. Chaque nuit, des données stratégiques et technologiques sont volées par milliers de gigabits, à des milliers d'ordinateurs appartenant à des entreprises occidentales.

- En outre, comme le secret de l'arme nucléaire en son temps, l'arme informatique est **discrète** et repose entre les mains de quelques individus. De plus, un manque de compréhension des appareils informatiques qui se trouvent en leur possession fait de la grande majorité des gens des victimes idéales. Pourtant, le piratage peut causer des **dégâts importants, durables, à une très grande échelle et à un coût dérisoire** pour ses auteurs. Il est de nos jours plus facile et moins coûteux de planifier un piratage contre quelqu'un que d'acheter une arme à feu. Face aux réductions de coûts et aux pressions en faveur des réductions du budget de la Défense, la guerre informatique devient, pour toute organisation malveillante, une option viable, et même alléchante.

- Pour terminer, la plupart du temps, le piratage n'est pas revendiqué. Il est très complexe d'en identifier l'auteur et les seules pistes possibles reposent sur des éléments de preuve concordants, la langue utilisée, des noms de commandes, et ainsi de suite.

Les piratages les plus ravageurs que l'on ait identifiés ont eu lieu au Moyen-Orient.

Cela commença en juin 2010 avec **Stuxnet.** Stuxnet semble avoir été le premier logiciel malveillant à cibler des infrastructures informatiques clés bien déterminées. Il avait pour but de s'attaquer aux centrifugeuses des usines d'enrichissement de l'uranium. Ce virus sophistiqué se propageait via les clés USB et profitait de failles de Windows ou de type « zero-day » pour s'installer. Par le biais de certificats numériques volés, Stuxnet avait pour cible les systèmes de surveillance et d'acquisition des données (SCADA) contrôlant les processus industriels et il avait pour but d'infecter les systèmes de contrôle à logique programmable (PLC).

D'autres vers destinés à des opérations d'espionnage, tels que **Dugu** et **Gauss**, découverts fin 2011, volaient les données et les mots de passe et installaient des portes dérobées. **Mahdi** et **Flame**, des logiciels malveillants plus insidieux, découverts début 2012, étaient aussi conçus pour l'espionnage.

Le dernier piratage connu, **Shamoon,** ciblait la grande compagnie nationale saoudienne Aramco. Cela commença par de la propagande sur des réseaux sociaux (Facebook, Twitter), quelques jours avant le piratage. Le 15 août, Aramco se déclara victime d'une entreprise de piratage à grande échelle qui, du jour au lendemain, détruisit complètement 30 000 disques durs d'ordinateurs. D'après les experts, cette opération de sabotage a été beaucoup plus facile à entreprendre que celle de Stuxnet, parce que le logiciel malveillant n'a pas eu à rester longtemps caché. Cela signifie que c'est une chose qui peut arriver à toute entreprise, à tout moment, sans prévenir. Shamoon était conçu pour frapper à un moment précis, et pour être relayé par une forte propagande. Par la suite, une offensive majeure par **déni de service** frappa les sites Internet de 20 banques américaines, dont des millions de demandes, de messages électroniques et de spams simultanés mirent les serveurs en panne (déni de service distribué).

Imaginons à présent une offensive contre des raffineries dans une grande ville portuaire. Tous les instruments de navigation sont bloqués. Impossible d'appeler les pompiers et les secours. Et en même temps, les réseaux bancaires sont piratés. Les pirates créent la panique et le chaos.

Un scientifique[1] a même prouvé récemment que les stimulateurs cardiaques radiocommandés peuvent être piratés par un virus et causer la mort subite de leur porteur, par choc électrique. Pire encore, ces virus peuvent s'étendre à d'autres porteurs et les tuer aussi. Ce n'est plus de la science-fiction, c'est notre réalité d'aujourd'hui.

Se pose alors la question suivante :

Les États sont-ils prêts à répondre à de telles menaces ?

Heureusement, il existe déjà des réponses.

Certaines concernent le **renforcement de la cybersécurité**, telles que **:**

- L'ouverture à Tallin du Centre d'excellence pour la cyberdéfense en coopération (CCDOE) accrédité par l'OTAN, après les attaques informatiques contre l'Estonie et les émeutes lors du déplacement du Soldat de bronze. C'est avant tout un centre de recherche juridique, non orienté vers l'action de terrain. On y compte à ce jour 11 pays[2], auxquels la France s'ajoutera bientôt.
- En outre, depuis juillet 2011, la France a mis en place sa propre Agence nationale pour la sécurité des systèmes d'information (ANSSI).

Un autre **moyen de lutter : investir dans des structures informatiques.**

- En 2010, les États-Unis ont mis en place la commande centralisée de leurs opérations informatiques, organisé les ressources informatiques existantes et synchronisé la défense des réseaux militaires américains.
- Israël a créé son Bureau informatique stratégique, qui collabore avec l'« Unité 8 200 » basée dans le désert du Néguev et travaille sur la cyber-sécurité des infrastructures centrales afin de contrer le cyber-terrorisme et d'identifier les failles des systèmes clés : notamment les réseaux informatiques des systèmes bancaires, des centrales énergétiques et d'autres infrastructures civiles.

Ces exemples témoignent d'une bonne volonté et d'une évolution culturelle infléchissant l'état d'esprit militaire habituel.

Mais une autre question se pose :

Y a-t-il une doxa stratégique ?

La réponse à cette question n'est pas si claire. Bien entendu, des idées issues de cellules de réflexion ou du cyber-commandement américain, tels que le *Manuel de la guerre électronique* (*Manual for Cyber Warfare*[3]) ou le *Manuel de Tallin*[4] de l'OTAN, fournissent des pistes intéressantes. Mais un agenda de mesures réelles, basées sur une doctrine, ne semble pas exister sur le long terme.

---

1 Barnaby Jack d'*IO Active,* à la Conférence Breakpoint sur la sécurité en 2012.

2 L'Estonie, l'Allemagne, l'Italie, la Lettonie, la Lituanie, la Pologne, la Slovaquie, l'Espagne, la Hongrie, les États-Unis et les Pays Bas.

3 Le manuel pratique FM 3-36 présente la doctrine de l'armée américaine de planification, de préparation, de mise en place et d'évaluation de la guerre électronique afin de renforcer l'ensemble des opérations terrestres. Ce manuel est destiné aux membres de l'armée à divers échelons et postes de commandement. Il fait autorité auprès du personnel chargé de mettre en place : la doctrine (principes fondamentaux, techniques et procédures), le matériel et la structure des forces ; la formation institutionnelle et l'entraînement d'unités ; les procédures standard pour le fonctionnement des unités ; et auprès du personnel qui planifie, prépare, conduit et évalue la guerre électronique.

4 Publié en novembre 2012 et rédigé sur la recommandation du Centre par un « groupe d'experts internationaux », ce manuel est le résultat de trois ans d'efforts pour déterminer dans quelle mesure les normes légales en vigueur s'appliquent à cette nouvelle forme de guerre. Le Manuel de Tallin accorde une attention particulière au *jus ad bellum,* le droit international qui régit le recours des États à la guerre comme instrument de politique nationale, et au *jus in bello,* le droit international relatif à la conduite des conflits armés.

Il serait sage de ne pas cultiver une mémoire défaillante et une vue à court terme. Chaque offensive provoque des réactions différentes et entraîne la mise en place de mesures et de stratégies spécifiques. Depuis Shamoon, l'opinion publique a pratiquement oublié les événements de 2007 en Estonie. Nous devons nous montrer très vigilants, car une offensive de piratage peut s'avérer aussi soudaine et traumatisante qu'elle peut également passer inaperçue sur une longue durée.

Le problème principal dans la guerre électronique est une **crise de confiance** dans nos systèmes informatiques. Sans même parler d'un dysfonctionnement des SCADAS (systèmes de surveillance et d'acquisition des données), qui serait le pire scénario. Le piratage d'une banque ou d'un site de sécurité sociale sonnerait le glas de la confiance des clients, utilisateurs et citoyens de nos sociétés modernes. L'autorité de l'état, soumise à la pression du mécontentement et de la méfiance des citoyens, serait remise en question. Étant donné que nous dépendons de plus en plus des technologies que nous utilisons dans tous les domaines liés à notre environnement économique et social, il devient beaucoup plus facile que nous le pensons de mettre fin à notre monde. Nous sommes menacés par une crise de confiance mondiale qui nécessite une prise de conscience et une vigilance constante afin d'être évitée.

Merci.