CYBER ESCARMOUCHES OU ÉTAT DE CYBERGUERRE, UN RISQUE MAJEUR

Par Gérard Peliks
Président de l'atelier sécurité de Forum ATENA
Intervenant dans des Mastères spécialisés de l'ISEP

Cet article est paru dans le numéro 104 de Signaux, la revue d'ISEP Alumni, « Le management du risque » daté du 16 janvier 2013.

Il est reproduit avec l'aimable autorisation d'ISEP Alumni.

L'information, les systèmes d'information, les réseaux connaissent aujourd'hui des attaques répétées, de plus en plus violentes, exécutées par des vecteurs très sophistiqués. Ces attaques n'ont pas pour but la recherche d'un gain pécuniaire mais plutôt tentent de dérober des informations sensibles ou de compromettre les infrastructures vitales des pays ciblés. On ne parle pas alors de cybercriminalité, ce sont les pays et leurs citoyens, les entreprises et leurs employés qui sont visés. Mais peut-on pour autant qualifier cet état de « cyberguerre » ? La guerre dans le cyber espace aura-t-elle lieu ?

Plus un pays est avancé dans l'utilisation des technologies du numérique, plus il est fragilisé, car le combat, au moins aujourd'hui, est un combat asymétrique où le faible peut faire d'autant plus de dégâts chez son adversaire qu'il est fort. A ce risque s'ajoute bien sûr la possibilité pour le fort de répliquer par des représailles qui sortent du domaine de la guerre virtuelle.

2012 est l'année de tous les dangers. Tout s'accélère côté attaques menées par des maliciels très sophistiqués, mais revenons d'abord quelques années en arrière.

2007, l'Estonie, un des pays les plus avancés en Europe dans l'utilisation des technologies du numérique par sa population, a été la cible d'attaques simultanées en dénis de services distribués (DDOS), provenant de plusieurs dizaines de pays, et qui ont abouti à l'isolement de cet état et à l'impossibilité pour les Estoniens d'accéder à leurs administrations, à leurs services bancaires, aux services de télécommunication et aux numéros d'urgence. Que s'était-il passé ?

On a pu constater que ces attaques avaient été déclenchées suite au déplacement, à Tallinn, d'une statue érigée à la mémoire du soldat soviétique lors de la deuxième guerre mondiale. Cette action déplut fortement à la communauté russophone d'Estonie. Des sollicitations multiples vers les serveurs Web estoniens affluèrent de toutes parts jusqu'à bloquer complètement les systèmes d'information du pays. Mais pourquoi ces sollicitations sont-elles venues simultanément de nombreux pays qui n'avaient rien à

voir avec les relations russo-estoniennes ? La technique utilisée fut celle des « botnets », ces ordinateurs ou réseaux d'ordinateurs, situés un peu partout dans le monde, infectés par un virus et devenus zombies. Ils obéissaient à distance aux ordres de serveurs, dits de « Command & Control », commandités, pense-t-on, soit par des groupes autonomes de pirates russophiles, soit par des groupes de pirates contrôlés par l'État russe, le saura-t-on avec assurance un jour ? Ces serveurs « Command & Control » commandaient aux ordinateurs zombies, à l'écoute de leurs ordres, de lancer des sollicitations vers les serveurs Web estoniens. Les botnets, ces armes de perturbation massive, ont ainsi fait du cyberespace un remarquable vecteur de nuisance des états attaqués.

En 2008 éclatait un conflit entre la Russie et la Géorgie, la Russie souhaitant récupérer l'Ossétie du Sud. Suite à des manifestations hostiles de la Géorgie, l'armée russe a pénétré en Ossétie sans que la Géorgie puisse réagir efficacement, car ses systèmes de communication et d'information stratégiques avaient été complètement bloqués au moment de l'attaque russe. De plus, les Web institutionnels géorgiens avaient été défigurés pour donner une image négative du pays assailli. Là, on a vu de vrais tués, pas seulement des cybertués comme dans les jeux vidéo. Ce n'étaient pas, bien sûr, des bits à 0 ou à 1 qui ont tué, ce sont les bombardements, mais les victimes auraient pu être ailleurs si elles avaient pu obtenir les bons renseignements au bon moment. Le monde était entré dans l'aire d'un conflit qui s'appuyait sur la destruction des ressources numériques de l'adversaire, avant de l'abattre.

Cette même année, Conficker, ver particulièrement prolifique, envahissait l'Internet et attaquait les serveurs qui avaient eu la malchance de se trouver sur son passage, en multipliant les processus dont l'accumulation bloquait leurs capacités de calcul. Beaucoup d'ordinateurs en ont fait les frais. Les aéronefs de certains pays furent bloqués au sol, ou sur leurs plateformes en mer, faute de pouvoir télécharger leurs paramètres de vol. Les réseaux militaires sensibles infectés par le ver Conficker étaient-ils connectés à l'Internet ? Non bien sûr, mais par une clé USB, on transfère facilement un fichier infecté d'un réseau public vers un réseau privé et même confidentiel.

En 2010, il y eut un fait nouveau qui allait populariser un danger auquel tout pays est maintenant exposé : un ver s'attaquait à des infrastructures sensibles très ciblées ! Stuxnet, c'est son nom, fut introduit sur un des serveurs Windows de l'usine d'enrichissement d'uranium de la centrale de Natanz, en Iran. Bien entendu cette infrastructure sensible n'était pas connectée à l'Internet, mais une clé USB ou une barrette mémoire infectée firent l'affaire. Aussitôt le ver se répandit sur les autres serveurs Windows du complexe industriel à la recherche d'un type précis d'automate programmable Siemens connecté au réseau. Ces automates programmables régulaient la vitesse de rotation des centrifugeuses qui servaient à enrichir l'uranium. Un coup Stuxnet faisait tourner les centrifugeuses plus vite, un coup moins vite, un coup elles s'arrêtaient et puis on repartait. Les centrifugeuses ont dû sacrément vibrer et chauffer… Mais les tableaux de contrôle auraient dû s'en apercevoir et sonner l'alarme ! Non, car le ver, qui connaissait les signaux qui étaient envoyés quand tout tournait de façon nominale, les transmettait aux salles de contrôle à la place des vrais signaux d'alerte, pour que les dispositifs de contrôle ne s'inquiètent pas. Bilan : un millier de centrifugeuses détruites et le programme nucléaire iranien arrêté pendant plusieurs mois. Ce ver a popularisé les attaques dites « contre les architectures SCADA (Supervisiory Control and Data Acquisition) ». Avec 4 000 fonctions différentes, l'exploitation de quatre failles non connues, donc sans correctif, dites « failles 0day », utilisant des logiciels signés (par des certificats volés), donc n'éveillant pas la curiosité des défenses des systèmes attaqués, Stuxnet ne pouvait être que créé par une ou plusieurs nations très évoluées et très portées dans la confection de maliciels. Qui était l'agresseur ? Maintenant on le sait, les USA et Israël avaient conçu ce ver très élaboré. Mais suite à un bug, Stuxnet est sorti de l'usine de Natanz dans l'ordinateur d'un chercheur iranien pour parcourir le monde. Il s'est répandu dans de nombreux pays et il a été découvert. Stuxnet ne constitue-t-il pas, là encore, un acte de guerre ? D'autant plus qu'en parallèle à l'attaque de Stuxnet, certains chercheurs iraniens travaillant dans l'industrie nucléaire ont connu une fin tragique.

En 2011, en France, le Ministère de l'Économie et des Finances, ainsi qu'Areva et sans doute beaucoup d'autres entités manipulant des informations très sensibles, ont subi des attaques dites « en APT » (Advanced Persistent Threats). L'attaquant prend connaissance à distance du système d'information et des habitudes des employés de la cible. Au bout de plusieurs mois, par des scans réseaux, par les réseaux sociaux, par des indiscrétions de toutes sortes collectées par téléphone, l'attaquant a constitué une connaissance approfondie de la topologie du réseau cible et des habitudes de ceux qui l'utilisent. Il ne s'agit pas là d'une attaque à l'aveuglette par des virus, les futures victimes sont très ciblées. Un employé, haut fonctionnaire dans le cas de Bercy, reçoit un e-mail provenant d'une origine qui lui inspire confiance (il ne devrait pas). Cet e-mail contient en attachement un fichier, par exemple PDF, à ouvrir de suite. Le PDF ouvert contient le ver qui s'introduit sur son système, capture identifiants et mots de passe, augmente ses privilèges et se répand, par le réseau sur d'autres calculateurs ciblés. Le ver est dans le fruit ! Ensuite, le ver établit un canal de diffusion vers un serveur de « Command & Control » qui va récolter les informations que les postes de travail compromis chiffrent et transmettent. A Bercy, 150 postes de travail ciblés, parmi les plusieurs dizaines de milliers du Ministère, transmettaient ainsi des informations sensibles vers l'étranger (vers la Chine) et cela pendant plusieurs mois. Les secrets du G8 et du G20, dont la France avait la présidence, ont ainsi quitté Bercy. L'ensemble des attaques en APT auraient fait perdre au pays 1% de son PIB. Qu'un pays subtilise les informations sensibles d'un autre pays, nuisant ainsi à sa souveraineté, n'est-ce pas un acte de guerre constitué ?

ARRIVE 2012, ANNÉE DE TOUS LES DANGERS.

Ce début d'année a vu le déchainement des Anonymous sur la toile mais on parle là plutôt de cyber hacktivisme, pas de cyberguerre, puisqu'aucun pays en particulier n'était censé être l'agresseur. Parmi les agressés il y eut tout de même en France le site de l'Élysée et ceux de plusieurs ministères. Les Anonymous protestaient contre la fermeture de MegaUpload et contre le fait que les officiels français approuvaient cette fermeture.

Plus en rapport avec notre sujet, en avril 2012, le virus Wiper attaqua les bases de données servant à la gestion portuaire du terminal de Kharg en Iran, seule porte encore ouverte pour exporter leur pétrole malgré les embargos. Des bases de données et de nombreux fichiers indispensables aux échanges commerciaux furent corrompus. Le ver Wiper s'est montré particulièrement destructeur et les exportations de pétrole iranien ont été bloquées. L'Iran a été encore un peu plus asphyxié par cette agression caractéristique d'une cyberguerre déclarée.

Mais ce n'était pas la dernière cyberattaque qui allait s'abattre sur ce pays, en cette année 2012. Duqu (prononcez Diouquiou), un ver avide en collecte d'informations sensibles, s'est intéressé aux ordinateurs détenus par des personnes ciblées en Iran, au Soudan et dans d'autres pays de la région. Duqu renvoyait les contenus des serveurs piratés à des serveurs de « Command & Control » en Allemagne et au Vietnam. Sitôt découvert, sitôt analysé, Duqu contenait des parties de codes communes avec Stuxnet, le ver qui avait attaqué les centrifugeuses du complexe de Natanz, deux ans auparavant. Mais de là à dire que Duqu était postérieur à Stuxnet, il y a un pas qu'il ne faut pas franchir. Qui connait la date exacte de début de l'agissement d'un maliciel qui peut dormir plusieurs mois avant de se réveiller et agir ?

En juin 2012, le ver Flame fut décelé sur des systèmes d'information de l'Iran et d'autres pays de la région où il sévissait depuis plusieurs années déjà. Cette boîte à outil d'espionnage très sophistiquée, totalisant tout de même vingt mégaoctets de code, installée en tout ou partie sur un poste de travail, écoutait sur les postes de travail infectés, les frappes clavier, faisait des copies d'écran, recherchait des fichiers « Autocad » qui sont en général des plans de lieux stratégiques. Flame parvenait aussi par Bluetooth, à allumer les téléphones portables à proximité des ordinateurs infectés pour écouter les conversations environnantes et même activer leurs caméras. Flame partageait aussi des portions de code avec Stuxnet et Duqu, et utilisait les mêmes vulnérabilités des machines cibles pour se propager. Alors si vous passez par cette région, méfiez-vous de votre Smartphone si vous l'utilisez pour des activités que vous voulez garder pour vous. Votre Smartphone n'est peut-être pas seulement l'objet indispensable pour rester connecté à l'Internet, mais peut devenir un sacré petit bavard et un vilain espion qui relate tous vos actes et paroles, vous qui sans le savoir êtes au beau milieu d'une cyberguerre qui fait rage ! Il ne s'agit pas alors de jouer les héros mais plutôt de vous poser la question « Est-ce cela une bataille ? » comme l'aurait fait un Fabrice Del Dongo dans une Chartreuse de Parme des temps modernes. Et quand Flame fut découvert, il s'est autodétruit, obéissant à une commande venue de l'extérieur. Ainsi cette cyberarme n'a pu être pleinement analysée, et donc reproduite, par les agressés pour répondre aux agresseurs par une autre cyberarme inspirée de la première.

Mais la réponse de l'Iran ne tarda pas à venir avec le virus Mehdi, en juillet 2012, qui s'attaquait à des ordinateurs Israéliens pour leur subtiliser des données sensibles.

Et en cet été 2012, le virus Gauss fit son apparition dans le cyberespace, lui aussi cheval de Troie ultra sophistiqué qui se mit à espionner les ordinateurs des banques libanaises, des banques des territoires palestiniens et bien sûr aussi celles de l'Iran. Était-ce pour déceler des transferts de fond pour l'achat d'armes non conventionnelles par des pays ou des mouvements terroristes ? Là encore nous sommes au cœur d'une cyberguerre. De plus, Gauss peut muter et attaquer les infrastructures sensibles des pays ciblés. A la différence de Flame qui se détruisait sur commande à distance, Gauss se supprimait après trente exécutions. Et quand on constate que Stuxnet, Duqu, Flame et Gauss partagent des portions de code en commun et utilisent parfois les mêmes vulnérabilités des logiciels des ordinateurs cibles pour se propager, on peut émettre des hypothèses sur les auteurs.

Le degré de sophistication et les ressources considérables nécessaires pour le développement de telles cyberarmes, ne peuvent être que le fait de pays. Georges Bush puis Barack Obama ont toujours été favorables à l'utilisation du cyberespace comme théâtre de lutte (opération « Olympic Games ») dont quatre vecteurs (Stuxnet, Duqu, Flame et Gauss), quand ils ont été découverts, étaient en activité depuis déjà plusieurs mois, peut-être depuis plusieurs années. Il faut aussi compter ce qui n'est pas encore découvert et qui est sans doute la partie cachée de l'iceberg.

PEUT-ON GAGNER UNE GUERRE EN LA MENANT SEULEMENT DANS LE CYBERESPACE ?

Je ne pense pas. De même que les bombardements allemands sur la Grande Bretagne en 1940 ou les bombardements des alliés sur l'Allemagne en 1944 n'ont pas suffi à entrainer la reddition de l'adversaire, la destruction des systèmes d'Information et de Télécommunications, et plus généralement la compromission des infrastructures sensibles, peut causer un effet de nuisance extrême sur un pays mais

ne peut le contraindre pour autant à se soumettre à la volonté du vainqueur. Pour vaincre, si tel est le but, une agression physique dans le périmètre terre/air/mer/espace doit suivre les effets obtenus par le cyberespace.

LA CYBERGUERRE PEUT-ELLE CONSTITUER UN ÉTAT DE GUERRE ?

La question mérite d'être débattue. Il est sûr que si une guerre implique l'usage de la force, tant qu'on reste dans le numérique, les dégâts sont visibles mais où est « la force » ? La cyberguerre est plutôt assimilable à ce qui se passait durant la guerre froide. Des escarmouches, un espionnage exacerbé de tous les côtés, mais pas d'invasion brutale du territoire adverse. On possède des armes de destruction massive mais on ne les utilise pas, par peur des représailles. Certes la destruction de l'infrastructure électrique d'un pays paralyserait totalement le pays agressé. Et plus le pays est évolué, plus il a à craindre une telle éventualité, surtout les pays qui, par l'Internet, régulent l'offre en énergie avec la demande des foyers, comme aux États-Unis avec les Smart Grids. Mais qui franchirait la ligne rouge au risque de déclencher les foudres de l'adversaire, et pas seulement dans le cyberespace, et pas seulement avec des armes virtuelles ?

Le risque est donc accru depuis qu'aux champs de bataille classiques s'est ajouté le cyberespace. Plus que jamais, et l'année 2012 le justifie, entre paranoïa collective et insouciance, mieux vaut renforcer la cybersécurité au niveau de toutes les infrastructures vitales d'un pays et se tenir au courant du développement des cyberguerres qui font rage dans le cyberespace.

A PROPOS DE L'AUTEUR

Gérard Peliks est expert sécurité chez Cassidian CyberSecurity. Cassidian est la division « Defense and Security » d'EADS, Cassidian CyberSecurity regroupe les activités « cyberdéfense » de Cassidian.

Il préside l'atelier sécurité de l'association Forum ATENA, et coordonne l'activité sécurité de l'Information du Cercle d'Intelligence Économique du Medef Île-de-France.

Il est chargé de cours sur différentes facettes de la sécurité, dans le cadre de mastères à Telecom ParisTech et dans d'autres écoles d'Ingénieurs. A l'ISEP, il intervient sur des modules sécurité dans le cadre des mastères spécialisés et a participé au comité de pilotage du Mastère Spécialisé en Intelligence des Risques et des Opportunités par l'Intelligence Économique.