CYBERESPACE

LA NOUVELLE GUERRE MONDIALE

Sites officiels piratés, programmes espions, virus... Invisibles, les frappes informatiques sont fréquentes et destructrices. Tous les pays s'arment pour se défendre... ou attaquer

PAR BORIS MANENTI ET JEAN-BAPTISTE NAUDET

MICHAEL FALCO/THE NEW YORK TIMES-REDUX-REA

A l'Académie militaire de West Point aux Etats-Unis, des cadets font des exercices pratiques de cyberattaques.

ISAAC BREKKEN-AP-SIPA/HO-AFP

Deux balles dans le cœur, à bout portant. A conflit moderne, vieilles méthodes. Assassiné récemment à coups de revolver dans un bois du nord-ouest de Téhéran, Mojtaba Ahmadi, commandant du quartier général de la cyberguerre de la République islamique d'Iran, est la première victime répertoriée d'une nouvelle guerre mondiale, secrète et vicieuse : la guerre informatique. Pour certains, ce conflit numérique serait même devenu la mère de toutes les batailles.

« Sera maître du monde celui qui sera maître de l'air », prédisait Clément Ader, ingénieur français et pionnier de l'aviation. Avant que le général italien Giulio Douhet ne fasse de la supériorité aérienne le pivot de toute stratégie militaire, puisque *« les bombardiers passent toujours »*. Des constats du XXe siècle aujourd'hui obsolètes. A l'heure où téléphone, montre, voiture et même compteur électrique se connectent à internet, *« le cyberespace n'est-il pas appelé, à son tour, à dominer les autres éléments, terrestre, maritime et aérien ? »* s'interroge Michel Baud, officier de l'armée de terre et chercheur à l'Institut français des Relations internationales (Ifri).

Parallèlement au cyberespionnage, la question du champ de bataille numérique se fait de plus en plus prégnante pour les armées du monde entier. Aux Etats-Unis, pays le plus avancé en la matière, la défense et la guerre sont pensées dans tous les domaines : air, terre, mer, espace et cyberespace. Le président Obama peut ainsi mener non seulement des représailles mais aussi des frappes informatiques « préventives » dès lors que la Maison-Blanche dispose de preuves tangibles annonçant une cyberattaque d'envergure. Le tout en lien avec le Cyber Command, dirigé par le général Keith Alexander, chef de la fameuse NSA, qui *« conduit des cyberopérations militaires dans le but de permettre des actions dans tous les domaines »*.

Tester ses propres boucliers

Les Américains, comme les Israéliens, n'hésitent plus à développer des cyberarmes *(voir encadré)* capables de s'introduire dans les systèmes informatiques ennemis pour les espionner et/ou les détruire. Une puissance de feu numérique qui a pour conséquence la mise hors service de cibles réelles comme des radars et des moyens de communication ou d'approvisionnement en électricité. Les virus sont en passe de remplacer les bombardements afin d'accompagner les actions au sol. Avant un raid aérien sur la Syrie, Israël aurait ainsi lancé une frappe numérique pour détruire les radars et paralyser la défense antiaérienne adverse. Le développement de capacités offensives permet aussi de tester ses propres boucliers afin de ne pas être victime de cyberattaques semblables à celles conçues par ses équipes. D'autant que, dans le cyberespace, quelques hackers à la solde d'un Etat ou d'un groupe terroriste suffisent à mettre hors circuit plusieurs jours de suite un pays comme l'Estonie.

Tout commence en 2007, dans cette petite République ex-soviétique qui a déclaré son indépendance en 1991. Cette année-là, un conflit symbolique oppose le jeune Etat devenu hyperconnecté et high-tech à la Russie voisine, qui ne supporte toujours pas qu'il ait décidé de voler de ses propres ailes. Pour affirmer sa souveraineté, le gouvernement estonien fait enlever un monument à la gloire de l'URSS dans un jardin public de Tallinn, sa capitale. Alors que la tension est à son comble, une attaque bloque les réseaux informatiques des services publics mais

Le général Keith Alexander, chef de l'Agence de Sécurité nationale (NSA)

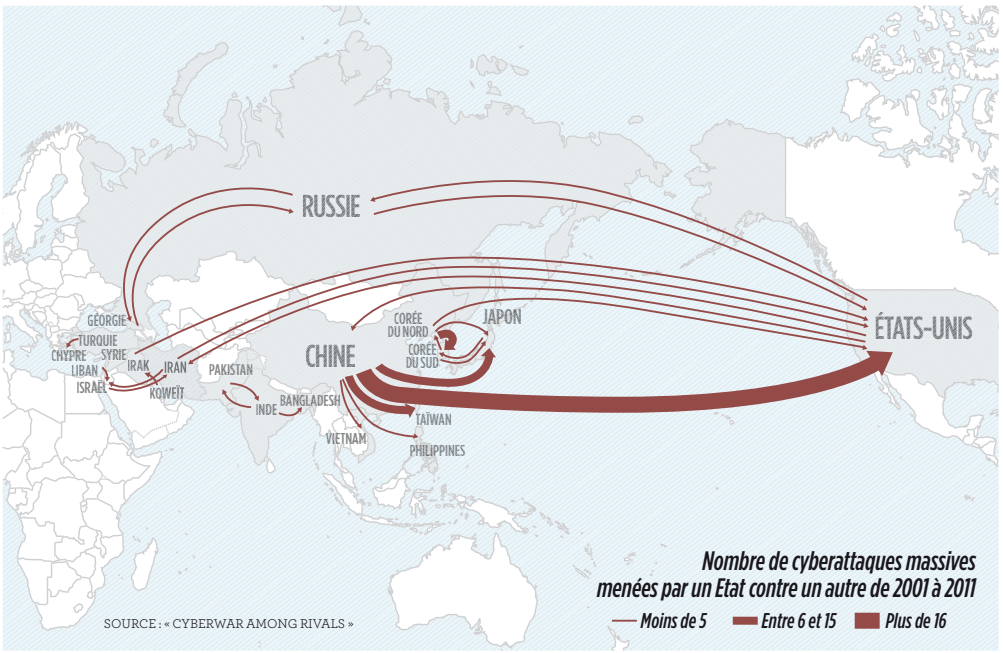
Le président Ahmadinejad, dans une usine d'enrichissement d'uranium, cible privilégiée de cyberattaques

aussi des banques et de tous les systèmes connectés, nombreux en Estonie. Le pays est paralysé. Cette attaque, même si elle utilise des ordinateurs « fantômes » contrôlés à distance depuis d'autres pays, a bien pour origine… la Russie. C'est la première fois qu'un conflit entre Etats tourne à la cyberguerre. Deuxième cible : la Géorgie, en 2008. Cette fois, la Grande Russie accompagne de frappes informatiques l'offensive de ses troupes et de ses chars. Les dégâts sont limités voire symboliques, car internet est peu développé dans la petite République du Caucase. Mais le pas est franchi : la guerre classique se double maintenant d'une guerre numérique. Et peut-être la précède, la remplace ou permet de l'éviter.

Conflit avec l'Iran

L'exemple de l'Iran, où la cyberguerre est sans doute la plus acharnée, est parlant. Alors qu'Israéliens et Américains menacent de bombarder les installations nucléaires de Téhéran pour l'empêcher de se doter de la bombe atomique, le conflit fait déjà rage dans le cyberespace. En 2010, Stuxnet, un programme malveillant, sans doute coproduit par les services américains et israéliens, a notamment été introduit dans les systèmes informatiques contrôlant les centrifugeuses qui enrichissent l'uranium nécessaire à la fabrication de l'arme atomique. L'opération a été renouvelée en 2012, avec un autre programme, espion cette fois-ci, Flame. Bilan : des centrifugeuses endommagées, parfois détruites. Certaines auraient même explosé. De quoi, peut-être, laisser le temps aux diplomates occidentaux de convaincre les Iraniens de renoncer à leurs projets atomiques. Et éviter une guerre, cette fois à coups de missiles.

Si, au Proche et au Moyen-Orient, la cyberguerre oppose essentiellement le petit Israël, passé maître dans les technologies de pointe, à ses voisins arabes ou musulmans, une autre bataille numérique, tout aussi virulente, fait rage entre les deux nouveaux géants mondiaux : les Etats-Unis et la Chine. Mais la très secrète unité chinoise « 61398 » serait essentiellement affectée au cyberespionnage économique et militaire. Car Pékin sait que, s'il veut dominer les Etats-Unis et le monde, il doit absolument combler son retard technologique. Pour gagner ce pari économique, commercial, numérique, la Chine a fait le choix de… voler les secrets occidentaux. Une méthode à bas coût, qui peut rapporter gros, et ce, apparemment, sans danger. Mais la guerre informatique, comme tous les conflits limités, peut dégénérer. En réponse à une cyberattaque affectant « leur existence », les Américains ont même récemment menacé de répliquer avec l'arme atomique. ■



LA COURSE AUX CYBERARMES

— En plein scandale des écoutes, l'Agence de Sécurité nationale (NSA) américaine vient de conclure un étrange contrat avec une entreprise française, Vupen. Cette discrète société montpelliéraine s'est spécialisée, comme ses concurrentes américaines Exodus Intelligence ou Immunity, dans la recherche de vulnérabilités, c'est-à-dire de failles informatiques inconnues dans des logiciels. Ces vulnérabilités (dites *zero-day*) peuvent permettre de s'introduire frauduleusement dans les systèmes ciblés (on parle alors d'exploit) afin de voler des fichiers confidentiels, d'installer des mouchards ou d'inoculer un virus pour détruire les machines. *« Ce sont des sociétés qui fabriquent des armes informatiques, comme d'autres fabriquent des chars »*, résume Eric Filiol, directeur du laboratoire de cryptologie de l'école d'ingénieurs Esiea.

Ces entreprises vendent leurs découvertes aux agences de renseignement et au plus offrant ! Les Etats-Unis, la Russie, Israël, la Grande-Bretagne et la Chine sont les plus gros acheteurs, selon le « New York Times ». *« On est en plein dans la course aux cyberarmes, parce que celui qui contrôle la technologie contrôle la guerre de demain »*, ajoute Eric Filiol. A combien s'échangent ces révélations concernant des vulnérabilités ? Une source bien informée évoque des prix entre 50 000 et 100 000 dollars pour un exploit dans Word et *« jusqu'à 500 000 euros pour un "zero-day" dans Windows 8 »*. Sachant qu'une faille n'est détectée qu'au bout de 312 jours en moyenne, selon la société d'antivirus Symantec, cela laisse tout le temps nécessaire pour fomenter un piratage. En France, la création, la détention et la mise à disposition de virus informatiques *« sans motif légitime »* s'apparentent à du recel : cinq ans de prison et 375 000 euros d'amende au maximum. En attendant, Vupen assure ne vendre ses services *« qu'aux organisations membres de l'Otan, de l'Anzus* [zone Pacifique] *et de l'Asean* [zone Asie] *et à leurs partenaires »*. De quoi se laisser une bonne marge de manœuvre. B. M.