29 avril 2012
Virus

Plongée dans les coulisses de la cyberguerre de l'ombre contre l'Iran

Ce dimanche 22 avril, les attaques informatiques perpétrées contre le secteur pétrolier iranien sont presque passées inaperçues. Pourtant, c'est une véritable guerre que se livrent Téhéran et les puissances occidentales, dans un nouveau champ de bataille: le cyberespace...

Avec Vincent Eiffling

Dans le bras de fer politique qui oppose les puissances occidentales à l'Iran autour de son programme nucléaire controversé, les « théâtres d'opérations » sont multiples.

Le terrain diplomatique tout d'abord, comme en témoigne le caractère itératif des rencontres entre émissaires iraniens et leurs homologues du groupe des 5+1 (les 5 membres du Conseil de sécurité des Nations-Unies plus l'Allemagne), lequel rassemble les Etats en charge de la gestion des négociations sur le dossier nucléaire de Téhéran. Ces négociations sont infructueuses depuis maintenant presque 10 ans. Cela dit, les discussions perdurent, et à en croire les protagonistes tout espoir n'est pas vain. En une décennie cependant, les avancées technologiques effectuées par l'Iran ont progressivement fait pencher la balance en sa faveur. Pourquoi ? Parce que plus l'Iran assure sa mainmise sur la maîtrise des divers aspects de la technologie nucléaire, plus il sera difficile de l'y faire renoncer, chaque pas en avant constituant un acquis présenté comme une illustration de la grandeur de la nation iranienne par ses dirigeants. Le nationalisme, le populisme, et par-dessus tout la victimisation par rapport à ce qui est présenté comme une attitude « injustement belliqueuse » de la part des puissances occidentales, constituent autant d'ingrédients qui caractérisent la rhétorique d'un régime en mal de légitimité, qui s'identifie depuis plus de trente au travers de l'animosité qu'il éprouve à l'encontre des Etats-Unis, et plus largement de l'Occident.

Outre la diplomatie, **le domaine économique constitue également un terrain d'action propice dans la lutte contre les ambitions iraniennes.** En plus des 4 résolutions votées depuis 2006 par le Conseil de Sécurité, des sanctions unilatérales ont été prises aussi bien par Etats-Unis que par les Etats-membres de l'Union Européenne.

L'option militaire, bien que non encore mise en œuvre, constitue un troisième moyen d'action dont la crédibilité se doit d'être préservée si les puissances occidentales désirent être en mesure de faire plier l'Iran sur le terrain diplomatique.

Quatrième théâtre, mais non des moindres : **les opérations clandestines de terrain. Celles-ci se sont multipliées ces dernières années, comme en témoignent les assassinats de scientifiques iraniens travaillant dans le domaine du nucléaire.** En outre, d'autres faits troublant sont à mentionner comme l'explosion survenue le 12 novembre 2011 sur la base militaire d'Alghadir, près de Téhéran, suivie le 28 de ce même mois par une autre explosion survenue sur un site de recherche nucléaire situé à Ispahan. S'agit-il de l'œuvre du Mossad ? Cela ne fait pas de doute pour le régime iranien. Côté israélien en revanche, on se contente de déclarer, à l'instar d'Ehud Barack, que d'autres incidents de ce type sont toujours les bienvenus…

Le cyberespace, nouveau champ de bataille de la guerre Iran / Occident

Enfin, il existe un cinquième théâtre d'opération où s'affrontent l'Iran et ses plus virulents opposants : le cyberespace. L'avantage de celui-ci, c'est qu'il jouit d'un vide juridique complet. Rien ne codifie sur le plan international les agressions informatiques interétatiques. En l'absence de lois, l'état de nature prévaut et tous les coups sont permis. Dans ce jeu nouveau qui n'est rien de moins qu'un corollaire des avancées technologiques inhérentes à notre époque, l'avantage va à celui qui en maîtrise le mieux la substance. Inutile de préciser que le rapport des forces penche ici du côté occidental de la balance. **Le savoir comme les moyens dont disposent des Etats comme les Etats-Unis ou Israël sont sans commune mesure avec les ressources à la disposition de Téhéran.** Or depuis 2010, les attaques informatiques à l'encontre d'installations iraniennes ont connu une forte hausse.

Phénomène le plus médiatisé de cette lutte d'un genre nouveau, l'affaire Stuxnet, survenue en septembre 2010 et qualifiée de « véritable guerre électronique » par les dirigeants iraniens. Pour rappel, ce ver informatique s'était différencié de ses congénères par ses caractéristiques bien spécifiques. Il avait en effet été spécialement programmé pour s'en prendre à un certain type d'installations industrielles. Plus précisément, ce sont les installations pilotées par « Scanda », un système de contrôle mis au point et fourni par la firme allemande Siemens, qui constituaient la cible de Stuxnet. Se transmettant aussi bien par une simple clé USB que via un réseau interne, Stuxnet ne se contentait pas de voler des données. Il permettait littéralement une reprogrammation des infrastructures visées, tout en leurrant leurs superviseurs quant à l'état réel de leur fonctionnement. Au final, ce ver aurait infecté plus de 30 000 ordinateurs industriels en Iran et ses cibles principales n'ont été ni plus ni moins que les sites nucléaires de Busher (une centrale à eau légère – fournie par la Russie) et le site d'enrichissement d'uranium de Natanz. Sur ce dernier, Stuxnet s'est attaqué aux centrifugeuses iraniennes en en poussant les moteurs de rotor jusqu'à leurs fréquences de résonnances. Les vibrations ainsi engendrées en ont alors assuré la destruction. Au final, ce sont approximativement 1000 centrifugeuses qui ont été endommagées. Peu de temps après, selon un rapport de l'AIEA, seule 4000 centrifugeuses sur les 8000 que comptait à l'époque de site de Natanz se sont avérées être en fonctionnement. Quel est le poids de la responsabilité de Stuxnet dans cet état des faits ? Difficile à dire. **Les dirigeants iraniens, bien qu'ils aient admis la réalité de l'attaque, ont toujours cherché à en diminuer la portée.**

Quoi qu'il en soit, si Stuxnet n'a pas mis un coup d'arrêt au programme d'enrichissement iranien, et nonobstant le fait que sa portée demeure encore aujourd'hui difficile à évaluer, il n'en ressort pas moins une véritable volonté de la part des adversaires de Téhéran d'agir sur tous les fronts en vue de contrecarrer les desseins de la République islamique. Mais qui donc porte la responsabilité de cette attaque informatique ? **Selon le New York Times, Stuxnet serait le fuit d'une coopération américano-israélienne et aurait même fait l'objet de tests au cours de l'année 2009 dans le désert du Néguev, sur une cascade de centrifugeuses test.** Bien qu'ils ne soient jamais passés aux aveux, ni Washington ni Tel Aviv n'ont émis de démenti quant à une possible implication de leurs services, se contentant de constater que l'Iran rencontrait « des problèmes techniques ». Détail important : les installations nucléaires visées n'étaient pas connectées à internet. L'assistance d'un tiers – conscient ou non – a donc dû être requise sur le terrain afin d'infecter le premier ordinateur et ainsi permettre au ver de s'étendre sur le réseau interne.

Moins médiatisé que son grand frère, le virus Stars a frappé l'Iran en avril 2011, soit seulement 8 mois après l'éclatement de l'affaire Stuxnet. Cette fois-ci, bien qu'admettant quelques dégâts, les autorités iraniennes ont déclaré avoir repoussé l'attaque avec succès. **Il faut dire que Téhéran prend la menace au sérieux et s'est donc doté d'une unité, au sein des Gardiens de la révolution, en charge de la « guerre informatique ».** Les moyens de cette unité demeurent méconnus, mais à en croire les déclarations officielles, l'Iran serait fin prêt à mener le combat sur ce nouveau théâtre d'opération. Entendez par là que, partisan d'une posture défensive, Téhéran entend aujourd'hui passer à l'offensive. Il s'agit là d'une rhétorique propagandiste brassant des dires pour le moins peu crédibles aux yeux de l'observateur avisé. Les principaux faits d'arme iraniens dans cette « cyber-guerre » se résument pour l'heure au piratage ponctuel de quelques sites d'opposition au régime situés à l'étranger, tel que Voice of America. **Mais l'Iran a besoin de faire croire qu'il peut dominer en un tour de main n'importe quelle technologie**. Les exemples se comptent à foison. Comme lorsque Téhéran a déclaré en décembre 2011 que la capture sur son territoire d'un drône américain RQ-170 résultait d'une prise de contrôle à distance de l'appareil par une unité spécialisée qui l'avait par la suite forcé à se poser.

Alors que les Iraniens fanfaronnent, à l'instar du Général de Brigade Ali Fazli, en déclarant que la République islamique va prochainement se doter d'une « cyber-armée » composée de « milliers de hackers », il apparaît utile de souligner que la première des ressources dans ce nouveau type d'affrontement demeure la maitrise du savoir-faire. Etant donné leur retard dans ce domaine, il est pour l'heure difficile d'imaginer voir les Iraniens parvenir à faire jeu égal avec les Israéliens et les Américains du jour au lendemain. **La qualité du matériel mais aussi et surtout du personnel impliqué dans la lutte dans le cyberespace reste pour l'heure l'apanage d'un cercle restreint de pays dont l'Iran ne peut pas prétendre faire partie**, en dépit de ses envies. Ainsi, de l'avis d'experts, la programmation de Stuxnet, extrêmement complexe dans sa réalisation, aurait nécessité l'appui de seulement 6 à 10 développeurs accomplis sur une durée minimum allant de 6 à 9 mois.

Un parallèle peut être effectué entre les attaques contre l'Iran et la volonté affichée ces dernières années par l'Etat hébreu de donner un coup de fouet à ses capacités de guerre informatique. Depuis 2007, cette dernière constitue même l'un des piliers stratégique d'Israël. Tsahal dispose d'ailleurs d'une unité spécialisée dans les cyber-attaques : l'unité 8200. Pas plus tard que le 22 avril dernier, le Général Gantz admettait à l'occasion d'une interview que les opérations clandestines à l'encontre des ennemis d'Israël constituaient une constante de la stratégie de l'Etat hébreu, et que leur nombre allait croissant depuis le début 2012.

C'est dans ce contexte que s'inscrivent les attaques informatiques survenues le 22 avril dernier contre le secteur pétrolier iranien, sur lequel repose la survie économique du pays. Au regard de l'ensemble des cibles visées, l'objectif de ces cyber-attaques prises dans leur globalité présente une double finalité : il s'agit d'une part d'affaiblir économiquement et politiquement l'Iran, pour le forcer au compromis sur le terrain diplomatique tout en retardant d'autre part ses progrès dans le domaine du nucléaire, et repousser ainsi l'échéance au-delà de laquelle l'option militaire cesserait d'être une possibilité, pour devenir une nécessité.