



Les Israéliens sabotent dans l'ombre le programme nucléaire iranien. Un livre révèle quelques opérations exemplaires. Notamment l'"empoisonnement informatique" de l'Iran (*Les Guerres secrètes du Mossad*, d'Yvonnick Denoël)

Le compte à rebours est déclenché contre l'Iran à propos de son programme nucléaire, personne ne croit à sa vocation civile. D'un côté, la communauté internationale s'applique à durcir les sanctions financières et commerciales contre la République islamique, parce qu'elle refuse de respecter le traité de non-prolifération nucléaire qu'elle a signé. De l'autre, Israël parle d'une « menace existentielle » pour sa survie, tout en reprochant aux États-Unis et à l'Europe leur aveuglement. « L'Iran a franchi systématiquement les lignes rouges qui lui ont été imposées et bientôt il sera trop tard », s'alarment les responsables israéliens.

Israël est placé devant un choix stratégique lourd de conséquences. Soit il laisse agir la communauté internationale, en misant sur l'efficacité des sanctions pour affaiblir la volonté du régime iranien. Soit il précipite la décision par une frappe aérienne qui retarderait de quelques années la possession par l'Iran d'une arme nucléaire. Chaque option a ses contraintes et ses risques.

Le statu quo permet à l'Iran de progresser vers la réalisation de son projet pour être bientôt – fin 2012, 2013 ? – à l'abri de toutes représailles. Un raid aérien, compliqué mais à la portée d'Israël, embraserait évidemment le Moyen-Orient, notamment les régions pétrolières du Golfe, en "pourrissant" le retrait américain d'Irak, la sortie d'Afghanistan (3 400 Français) et la mission de paix des casques bleus de l'Onu au Liban (dont environ 1 300 Français). "Nous ne pouvons compter que sur nous et jamais plus la vie de juifs ne dépendra du bon vouloir des autres", disent en substance les Israéliens, au moment où la politique semble faciliter le recours à l'option militaire.

En attendant, Israël a déjà déclenché des opérations secrètes contre l'Iran, à coups d'assassinats ciblés et de sabotages techniques et informatiques d'une grande audace. C'est ce que raconte un ouvrage passionnant, à paraître ce 26 mai aux éditions Nouveau Monde, sous la plume d'Yvonnick Denoël, auteur spécialiste des questions d'espionnage. En voici quelques extraits sur la façon dont le Mossad israélien a réussi à "planter" l'informatique du programme nucléaire iranien. **Lire la suite**

Les Guerres secrètes du Mossad, d'Yvonnick Denoël, Nouveau Monde Éditions

" Lors de sa reconduction à la tête du service en 2007, après un premier mandat de cinq ans, Meir Dagan avait fait de l'Iran "sa" priorité. À l'époque, l'aggravation de la situation dans les territoires palestiniens et les surprises de la guerre du Liban en 2006 conduisaient à faire de l'Iran la cible privilégiée de ses efforts.

La défection d'Ali Reza Asgari, général des pasdarans passé au service de la CIA, fournit des éléments capitaux pour la suite des opérations. Vice-ministre de la Défense, Asgari avait été écarté du pouvoir après l'élection de Mahmoud Ahmadinejad à la présidence en 2005. Il livra des cartes militaires, le détail des installations nucléaires et de leur dispositif de sécurité (par exemple l'existence d'un second site nucléaire [clandestin] près de Natanz), les filières de livraisons d'armes au Hezbollah. Un mois après, ce fut au tour du consul d'Iran à Dubaï de faire défection : il livra d'importantes informations sur les opérations de déstabilisation des monarchies du Golfe.

Peu après, la série noire commença. Entre février 2006 et mars 2007, trois avions de la flotte des Gardiens de la Révolution s'écrasèrent. Chaque fois, ils avaient à leur bord des techniciens du nucléaire. L'état-major de la force terrestre des pasdarans fut même décapité dans l'un de ces crashes. Outre des assassinats ciblés de membres clés du programme iranien (ce volet restant le seul apanage du Mossad), Dagan mit en place bon nombre d'actions clandestines en partenariat avec les services américains, mais aussi allemands, britanniques et français.

Son plan prévoyait non seulement une audacieuse opération de cyberguerre, mais aussi le recrutement d'agents doubles, l'utilisation de sociétés écrans, et, selon un ancien de la CIA qui s'exprime sous condition d'anonymat, les services européens, américains et israéliens s'étaient concertés pour créer plusieurs sociétés commercialisant du matériel et des services à usage nucléaire. Ces sociétés avaient une véritable activité, chaque pays membre du programme veillant à leur fournir des marchés véritables. Elles utilisaient des équipes à plein temps, une

grande partie des employés ignorait d'ailleurs l'objet réel de leur travail. [...]

Les intermédiaires iraniens en charge de l'approvisionnement faisaient bien sûr l'objet d'une étroite surveillance des services. Lorsqu'on les pensait corruptibles, on tentait de les approcher pour les convaincre moyennant finances d'orienter leurs achats dans la bonne direction. S'ils ne l'étaient pas, c'était aux commerciaux de se débrouiller pour les séduire. [...]

Une fois le marché conclu, on commençait par livrer au client des matériels de bonne qualité, pour endormir sa méfiance. Ce n'est qu'après plusieurs livraisons que l'on glissait des composants et mécanismes subtilement modifiés pour poser des problèmes par la suite. Les vices cachés devaient rester indétectables pour ne pas "brûler" le fournisseur. Le deuxième objectif était ensuite d'obtenir un prétexte pour envoyer un représentant de la société sur un site du client, soit à des fins de maintenance technique, soit pour une visite commerciale.

Cette mission à haut risque avait pour but de prendre sur place des photos et recueillir d'autres éléments utiles, le tout sous bonne garde comme on s'en doute. L'information ainsi collectée était par la suite transmise aux services alliés et à l'Agence internationale de l'énergie atomique.

Une autre source, européenne cette fois, évoque le recrutement par le BND [service de renseignements allemand] en 2002 d'un homme d'affaires iranien dont l'entreprise participait à la construction de l'usine d'enrichissement d'uranium de Natanz. L'homme accepta de transmettre des plans et photos de l'usine, en échange d'une promesse de pouvoir fuir le pays et bénéficier de l'asile politique en Allemagne. Hélas pour lui, il fut démasqué et tout simplement abattu en 2004.

Son épouse, qui était dans la confiance, eut alors la présence d'esprit de quitter le pays en emportant l'ordinateur portable de son mari. Ce "sésame" contenait des centaines de documents que les services allaient mettre plusieurs mois à analyser.[...]

À la même époque, une série d'explosions et de morts mystérieuses frappa les sites de Natanz et d'Ispahan. Dès avril 2006, deux transformateurs avaient explosé lors de la première tentative d'enrichissement de l'uranium à Natanz – cinquante centrifugeuses furent endommagées.

Le 18 janvier 2007, le professeur Ar deshir Hassanpour, expert en électromagnétique travaillant sur le site d'Ispahan, fut retrouvé mort dans son appartement. Hassanpour était un physicien nucléaire de 44 ans qui travaillait à la production d'hexafluorure d'uranium, un gaz utilisé dans le processus d'enrichissement de l'uranium, notamment à l'usine de Natanz. Il avait reçu le grand prix de la Recherche militaire iranienne en 2004, ce qui en faisait un des scientifiques vedettes du pays. Sa mort fut annoncée en janvier 2007 comme la conséquence d'un « empoisonnement au gaz », sans plus de précision. [...]

L'usine de Dimona dans le désert du Néguev est bien connue pour abriter le centre stratégique des activités nucléaires israéliennes. Mais depuis 2009, elle hébergeait également une équipe de techniciens en lien permanent avec son homologue américaine : toutes deux étaient chargées de saper le programme nucléaire iranien.

C'étaient des tubes de 1,80 mètre de long et 10 centimètres de diamètre. Ils servaient à augmenter progressivement la proportion d'uranium 235, l'isotope fissile de l'uranium. Dans chaque centrifugeuse se trouvait un rotor qui tournait à 1 000 tours par seconde. En augmentant la fréquence à 1 400 tours par seconde, on pouvait faire exploser le tube. [...]

Selon un responsable du renseignement américain cité par le New York Times, c'est parce que les Israéliens ont pu le tester en situation réelle que le virus Stuxnet a été efficace. Pour conduire cette expérience, les services israéliens n'ont pas hésité à rappeler des techniciens et scientifiques à la retraite : ayant travaillé dans les années 1950 et 1960, ils étaient mieux à même de faire fonctionner du matériel ancien, au plus proche du savoir-faire iranien. Il fallut deux ans à l'équipe israélo-américaine pour développer Stuxnet et le rendre imparable. [...] L'idée était de retarder le programme iranien de plusieurs années, mais sans acte de guerre. Barack Obama fut informé de ce programme quelques jours avant de prêter serment et le confirma sitôt en poste. La conception informatique du virus lui-même allait résulter d'une collaboration entre le laboratoire du Home land Security (un laboratoire américain du département de sécurité nationale, créé dans la foulée des attentats du 11 septembre 2001) et une unité ultrasecrète de l'Aman dédiée à la cyberguerre.

En 2008, la société allemande Siemens avait accepté de coopérer avec Homeland Security, afin de lui permettre de rechercher les failles de ses ordinateurs utilisés par les Iraniens. Siemens fabrique en particulier des "contrôleurs", c'est-à-dire des ordinateurs qui gèrent le fonctionnement de vastes installations industrielles ou énergétiques. [...] Or il se trouve que ce sont des ordinateurs Siemens qui contrôlaient les installations de Natanz. [...]

Après une étude minutieuse, les chercheurs américains et israéliens mirent donc au point une forme primitive du virus, apparue sur le Web en juin 2009 sans que l'on puisse en identifier la source. [...]

L'action de Stuxnet consiste d'abord, comme pour un logiciel espion classique, à aspirer toutes les données disponibles sur la configuration de la machine et du réseau. Les données sont ensuite transmises à des sites en apparence anodins, hébergés pour l'un en Malaisie, pour l'autre au Danemark. Elles incluent les adresses IP des ordinateurs du réseau, leurs noms, systèmes, etc.

Quelques semaines plus tard, Stuxnet va prendre le contrôle d'une batterie de centrifugeuses, afficher sur les moniteurs de contrôle des signes d'activité "normale", tout en envoyant des instructions qui font accélérer et "dérailler" les centrifugeuses. Un peu comme ces cambrioleurs de banque qui connectent les caméras de surveillance à une vidéo montrant une salle des coffres déserte pour forcer les coffres en toute tranquillité. [...]

Le taux normal de "casse" dans une usine comme celle de Natanz, qui disposait de 8 700 centrifugeuses en 2009, ne devrait pas dépasser 10 % par an. Début 2010, les inspecteurs de l'AIEA comprirent que quelque chose clochait : en un trimestre les techniciens avaient dû remplacer entre 1 000 et 2 000 centrifugeuses ! [...]

Si le but de Stuxnet était de stopper l'enrichissement d'uranium et la production de bombes atomiques, il n'a pas été atteint. En revanche, l'opération a réussi, selon Meir Dagan, à repousser la production d'une arme nucléaire à 2015. Mais certains experts estiment cette affirmation trop optimiste. Il est confirmé que l'Iran a réussi à remplacer les 1 000 ou 2 000 centrifugeuses endommagées, donc la production d'uranium enrichi a pu reprendre. Et selon l'estimation de différents services, les Iraniens disposeraient encore d'une réserve de 8 000 centrifugeuses. "