Olympic Games : le cyberconflit contre le programme nucléaire iranien

Jean-Loup Samaan

En juin 2012, le journaliste du *New York Times* David Sanger révèle que le ver informatique Stuxnet qui a infecté à l'automne 2010 les centrifugeuses de l'usine iranienne d'enrichissement de l'uranium à Natanz était en fait la partie immergée d'un véritable iceberg : Stuxnet serait en réalité une composante des multiples opérations lancées clandestinement par les États-Unis dans le cadre d'un programme baptisé *Olympic Games* et datant de l'administration George W. Bush[1]. Au même moment, la société russe Kaspersky dévoile l'existence d'un virus Flame ayant infiltré les ordinateurs de hauts responsables iraniens depuis plusieurs années. Ces révélations constituent une étude de cas exemplaire sur l'emploi de cyber-attaques à des fins proprement stratégiques – en l'occurrence, décourager le régime iranien de poursuivre son programme nucléaire. Pour autant, une analyse approfondie des tenants et aboutissants de cette opération *Olympic Games* incite à la prudence, tant de nombreuses inconnues subsistent sur la logique de ce cyber-conflit.

Genèse d'*Olympic Games*

Selon les informations dévoilées aujourd'hui, la décision de la Maison Blanche de se lancer dans une vaste campagne de lutte informatique visant le programme nucléaire iranien aurait été prise courant 2006. La gestion diplomatique du dossier est alors dans une impasse : les négociations initiées par l'UE3 – regroupant le Royaume-Uni, la France et l'Allemagne – ont échoué l'année précédente et l'arrivée au pouvoir à Téhéran de Mahmoud Ahmadinejad en août 2005 est suivie d'une reprise de l'enrichissement de l'uranium en dépit des injonctions de l'Agence internationale de l'énergie atomique. L'administration Bush doit alors composer avec, d'un côté, un gouvernement israélien qui le presse de répondre avec dureté aux provocations iraniennes et, de l'autre, des alliés européens qui s'inquiètent des retombées de sanctions économiques sur leurs propres économies – en particulier la Grèce, l'Espagne et l'Italie, tous trois dépendant substantiellement des importations pétrolières iraniennes[2]. Alors que la guerre civile irakienne atteint son pic et achève de convaincre la Maison Blanche d'une augmentation nécessaire de ses forces militaires sur le théâtre – le fameux *surge* de 2007 –, l'option militaire vis-à-vis de l'Iran est pour l'heure écartée.

C'est alors que le général James Cartwright, à la tête du *Strategic Command* américain – en charge notamment de la gestion de l'arsenal nucléaire américain et du système de défense antimissiles – aurait réuni une *task force* composée des multiples agences de renseignement (au premier rang desquelles la *National Security Agency*) prônant auprès du chef de l'exécutif la conduite de cyber-opérations visant les installations principales du programme iranien.

Bush approuve l'initiative : c'est le début d'*Olympic Games*, la première grande entreprise moderne de cyber-opérations visant à mettre à mal le dessein proliférateur d'un État. Les débuts sont expérimentaux. Pour créer le programme informatique devant s'infiltrer dans le système d'information des usines

1. David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", *The New York Times*, 1 juin 2012.

2. Brandon Fite, *US and Iranian Strategic Competition: Competition Involving the EU, EU3, and non-EU European States*, Washington, Center for Strategic and International Studies, mars 2012, p. 19.

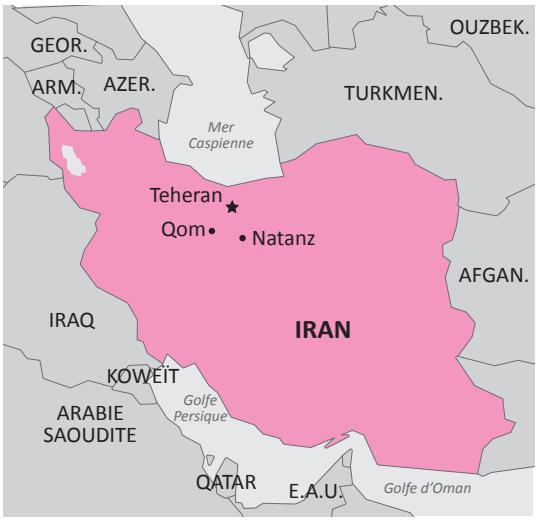
iraniennes, la NSA s'entraîne sur les centrifugeuses libyennes que le colonel Mouammar Gaddafi a remis à Washington en 2003 lorsqu'il a abandonné son propre programme d'armes de destruction massive. Les centrifugeuses libyennes comme iraniennes se trouvent en effet avoir un même concepteur : Abdul Qadeer Khan, « père » de la bombe nucléaire pakistanaise et patron jusqu'au début des années 2000 du plus grand réseau international de prolifération[3].

Dans les mois qui suivent, les cyber-attaques démarrent et des résultats, d'abord modestes, sont enregistrés par la NSA. L'effet recherché est délicat : il s'agit d'endommager les centrifugeuses iraniennes de manière à ralentir le programme, mais sans éveiller les soupçons des ingénieurs de l'usine de Natanz. Il semblerait ainsi que les scientifiques iraniens n'aient pas attribué les premiers dysfonctionnements à des intrusions étrangères, mais à de simples problèmes de maintenance. De plus, le programme informatique de la NSA a été configuré pour ne pas procéder deux fois de suite à une même attaque afin d'éviter un recoupement.

Lorsque George Bush quitte la Maison Blanche en janvier 2009, *Olympic Games* semble tout au plus être un outil de nuisance utile n'ayant pas empêché l'Iran de progresser dans le développement de l'enrichissement de l'uranium. Bush n'en est pas moins convaincu de la nécessité de poursuivre l'exploration de ce nouveau champ d'action et, lors de sa passation de pouvoir avec Barack Obama, il demande à ce dernier de ne pas démanteler deux programmes en cours : les frappes de drones orchestrées par la CIA dans les zones tribales du Pakistan visant les militants d'Al-Qaïda et les cyber-opérations contre le programme nucléaire iranien.

Dans les deux cas, Obama non seulement ne démantèle pas les initiatives prises par l'administration Bush, mais accroît leur champ d'action. C'est ainsi que le nouveau président, élu sur la promesse d'engager un dialogue sans précondition avec le pouvoir iranien, approuve le renforcement d'*Olympic Games* par la NSA.

Une des dimensions notables de cette montée en puissance du programme est la coopération technique extrêmement poussée entre Américains et Israéliens. En effet, les informations collectées par le renseignement militaire israélien sur Natanz se révèlent précieuses et permettent de réaliser des percées considérables dans la pénétration et l'endommagement des centrifugeuses.



Puis, au printemps 2010, le Pentagone et la CIA découvrent avec stupeur que la machine s'est emballée et que les cyber-attaques visant exclusivement les centrifugeuses iraniennes leur ont échappé : des ingénieurs iraniens de Natanz ont, sans le savoir, transporté un ver informatique de leurs terminaux de la centrale vers leurs ordinateurs personnels connectés à internet. Bientôt, le ver se propage sur la toile, contaminant près de 60 000 ordinateurs à travers le monde. Il éveille l'attention de Symantec et Kaspersky, les grandes compagnies de sécurité informatique. Les analystes en sécurité se montrent très rapidement surpris par le degré anormal de sophistication de ce programme qu'ils baptisent « Stuxnet ». À l'évidence, celui-ci n'a pu être conçu que par des services étatiques. De plus, le fait que 50 % des serveurs infectés soient localisés en Iran achève de convaincre la communauté informatique : Stuxnet est un logiciel dont l'existence ne devait pas être rendue publique et qui a été développé à des fins stratégiques extrêmement complexes – à savoir l'endommagement de centrifugeuses dont le

3. Sur l'histoire du réseau Khan, voir Bruno Tertrais, *Le Marché noir de la bombe*, Paris, Buchet-Chastel, 2009.

système d'information n'était pas relié à internet. Les soupçons se portent tout de suite vers les deux pays les plus actifs en matière de lutte informatique : les États-Unis et Israël. Le mobile politique est évident, tout comme les capacités de concevoir Stuxnet[4].

En cette fin 2010, malgré la spectaculaire couverture médiatique de Stuxnet, la Maison Blanche reste silencieuse. Rien ne doit laisser penser que l'administration Obama reconnaisse son engagement dans de telles opérations. Si une rumeur fait de Stuxnet un programme israélien[5], aucune déclaration officielle ne vient l'étayer. Il semblerait qu'au cours de cette période, Washington ait hésité à maintenir *Olympic Games*. Or, le rapport de l'AIEA sur le programme nucléaire iranien, qui sort quelques semaines plus tard, atteste d'un sévère ralentissement dans le rythme des centrifugeuses de Natanz. En d'autres termes, les cyber-attaques pourraient bien réussir à dissuader *in fine* le pouvoir iranien de poursuivre sa quête nucléaire.

Mais, encore une fois, les effets de ces cyber-attaques sont sujets à d'âpres débats. Les évaluations des dégâts causés par Stuxnet varient de telle façon qu'il est difficile de connaitre son exacte ampleur. Selon l'*Institute for Science and International Security*, près de 1 000 centrifugeuses auraient été remplacées entre la fin 2009 et le début 2010[6]. Le président iranien Mahmoud Ahmadinejad lui-même reconnait en novembre 2010 qu'un « nombre limité » de centrifugeuses a été atteint par le vers. Compte tenu de ces éléments prometteurs, Barack Obama décide alors de maintenir *Olympic Games*.

Premières leçons d'*Olympic Games*

Le timing des révélations sur ce programme de cyber-attaques américain dans le *New York Times* suscite de multiples controverses. Dans un premier temps, le Sénat dominé par les opposants républicains au président Obama accuse la Maison Blanche d'avoir orchestré les fuites délivrées au journaliste David Sanger afin de redorer son blason et de se construire une image « forte » sur les questions militaires à quelques mois d'une élection présidentielle qui pourrait s'avérer difficile pour le président sortant. Sanger s'en défend immédiatement, affirmant que, bien au contraire, la Maison Blanche aurait préféré poursuivre tranquillement, à l'ombre des regards de la presse, sa vaste entreprise de cyber-attaques.

Mais, plus encore que la scène intérieure, importe le contexte diplomatique dans lequel sont apparues ces révélations. L'article de Sanger paraît le 1er juin 2012, après une reprise des pourparlers diplomatiques entre l'Iran et les grandes puissances qui se sont réunis en avril à Istanbul et en mai à Bagdad. Le scandale se poursuit alors qu'une dernière réunion de haut niveau se déroule la deuxième semaine de juin à Moscou, qui échoue à son tour à obtenir une avancée.

En fait, rétrospectivement, *Olympic Games* pose ici une question cruciale : la Maison Blanche n'a-t-elle jamais cru au processus diplomatique avec les Iraniens ? Si l'enquête de Sanger est exacte – et, à ce jour, aucun élément n'est venu la démentir – ces attaques ont été menées alors qu'Obama faisait de l'*engagement* avec Téhéran la pierre angulaire de sa politique au Moyen-Orient.

Ironie de l'histoire, l'arrivée de Barack Obama à la Maison Blanche fin 2008 avait mis dans l'embarras ses partenaires européens. Alors que ceux-ci avaient adopté depuis deux ans une position ferme sur le dossier nucléaire iranien, Obama promettait de renouer des liens diplomatiques avec l'Iran sans condition préalable. Le revirement américain ne prenait alors pas en compte les propres conditionnalités de l'UE-3 dans les pourparlers avec les représentants iraniens. En effet, l'*engagement* d'Obama contredisait la position des Européens selon laquelle toute négociation devait être conditionnée par la suspension des activités iraniennes d'enrichissement et de retraitement de l'uranium. L'effet sur la cohésion du « camp transatlantique » fut notable et contribua en grande partie aux tensions

4. Sur Stuxnet, voir James Farwell, Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, vol. 53, n° 1, février-mars 2011 ainsi que le rapport official du Congrès, Paul Kerr, John Rollins, Catherine Theohary, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability", Congressional Research Service, décembre 2010.

5. Christopher Williams, "Israel video shows Stuxnet as one of its successes", *The Telegraph*, 15 février 2011.

6. David Albright, Paul Brannan, Christina Walrond, "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant?", ISIS Report, 22 décembre 2010.

diplomatiques entre l'administration Obama et la présidence de Nicolas Sarkozy.

Or, la nouvelle lecture qu'offrent les révélations de Sanger donne à voir un Obama beaucoup plus pragmatique, voire cynique, dans l'articulation d'une stratégique mêlant des messages diplomatiques bienveillants et un renforcement continu d'*Olympic Games*. À la lumière de ces événements, certains analystes sont même allés jusqu'à légitimer, *a posteriori*, le refus iranien de la main tendue d'Obama[7].

En fait, le programme *Olympic Games* a pu servir d'outil expérimental pour l'administration Obama estimant à la fois que le processus diplomatique était voué à l'échec en raison de la duplicité du régime de Téhéran et que des frappes militaires ne feraient qu'embraser la région. En d'autres termes, les cyber-attaques perpétuées par les États-Unis depuis 2008 ont permis de trouver une troisième voie, encore jamais inexplorée, dans la mise en œuvre d'une diplomatie coercitive[8].

Pour autant, cette voie reste bien expérimentale comme l'a révélé la propagation involontaire de Stuxnet à travers le monde au printemps 2010. C'est pourquoi, si *Olympic Games* met en lumière une nouvelle dimension de la lutte informatique à des fins stratégiques, son développement pose plus de questions qu'il n'apporte de réponses. À un premier niveau proprement politique, cette opération n'a-t-elle pas entériné le principe stratégique de cyber-attaques que les États pourraient conduire sans encombre juridique ? S'il s'agit bien là d'une troisième voie, à mi-chemin entre la diplomatie et la guerre, elle devient une option commode non seulement pour les Etats-Unis, mais également pour tous ses ennemis qui pourraient ainsi s'attaquer aux systèmes d'information américains en profitant de ce même statut ambigu. Le caractère littéralement hors-la-loi de ces attaques n'en est donc que plus préoccupant.

Une autre question proprement militaire découle de ces éléments : la gestion de l'escalade dans un tel conflit. Le récit de Sanger et les multiples révélations venues l'étayer décrivent une Maison Blanche tâtonnant dans l'obscurité, ne pouvant réellement évaluer les retombées de ses cyber-opérations : la grammaire de ce type d'affrontement clandestin n'existe pas à ce jour. Il en ressort le risque fort d'un dérapage incontrôlé – comme la propagation de Stuxnet le fut *a minima* – qui entrainerait les belligérants sur le chemin d'un conflit bien réel à la suite de cyber-attaques disproportionnées. Comme le soulignent deux chercheurs de King's College, Stuxnet était certes un ver extrêmement sophistiqué, mais ce n'était pas un agent évolutif. Stuxnet pouvait s'infiltrer et endommager les systèmes iraniens, mais il ne pouvait pas observer cet environnement, évaluer ses spécificités et évoluer en conséquence[9]. Une telle cyber-arme, capable d'adaptabilité dans le système ciblé, serait à n'en pas douter une arme magistrale, mais aussi une arme dont les effets sur l'escalade conflictuelle pourraient échapper à ses concepteurs.

De telles expérimentations pourraient *in fine* conduire les États à créer formellement ou informellement des règles pour maintenir la lutte informatique en deçà du seuil du conflit ouvert. On voit bien tout l'intérêt que des pays tels que les États-Unis auraient à contenir cette logique de l'escalade qui leur permet de bénéficier d'une option bien commode pour conduire une diplomatie coercitive. On a plus de mal à voir comment des pays tels que l'Iran pourraient accepter cette retenue en deçà du conflit ouvert. En effet, si un programme comme *Olympic Games* arrivait, à l'avenir, à endommager le programme nucléaire iranien dans des proportions qui se révélaient irréversibles pour les Iraniens, il n'est pas inutile de s'interroger sur les options de ripostes éventuelles que le régime de Téhéran pourrait alors envisager.

En somme, *Olympic Games* révèle tout autant qu'il obscurcit notre regard sur la lutte informatique et devrait, à cet égard, constituer une étude de cas particulièrement fertile pour les chercheurs au cours des prochaines années. ■

7. Voir, en particulier, Stephen Walt, "Breaking the golden rule", Foreign Policy Blog, 1er juin 2012. Consultable sur : http://walt.foreignpolicy.com/posts/2012/06/01/breaking_the_golden_rule_0.

8. Notion héritée de la guerre froide, la diplomatie coercitive s'appuie sur l'emploi de la menace ou de la force armée de façon graduelle et limitée afin de contraindre un adversaire.

9. Thomas Rid, Peter McBurney, « Cyber-Weapons », *RUSI Journal*, février-mars 2012, vol. 157, n° 1, p. 10.