Moyen-Orient : le « cyber », arme des États et d'autres entités

Au Moyen-Orient, zone conflictuelle, le « cyber » (ensemble de systèmes informatiques) permet aux acteurs étatiques ou non d'agir, de façon discrète et à faible coût, en matière de renseignement, de sabotage, d'opérations militaires, de communication, d'information et de simple attaque informatique.

Olivier Danino, chercheur à l'Institut français d'analyse stratégique, a présenté la situation au cours d'un séminaire organisé, le 21 mai 2014 à Paris, par l'Institut de recherche stratégique de l'École militaire. En outre, il a réalisé, pour le compte de la Délégation aux affaires stratégiques du ministère de la Défense, une étude rendue publique à cette occasion.

Principaux États. En matière de renseignement, les États recourent à la veille sur Internet (défense) et aux virus informatiques (offensive). Pays le plus en

avance du Moyen-Orient dans le domaine cybernétique, **Israël** veut créer une symbiose entre les mondes militaire, universitaire et industriel. L'accent est d'abord mis sur l'éducation de la jeunesse en la matière. Tsahal (forces armées israéliennes) finance une formation à l'informatique dans environ 50 écoles du pays depuis la rentrée scolaire 2012-2013 pour les jeunes de 14-15 ans et, avec d'autres organismes dont le ministère de l'Éducation, un programme d'expertise pour ceux de 16-18 ans. Plusieurs universités proposent des diplômes de cybernétique. Pendant leur service militaire, ces jeunes sont envoyés dans des unités spécialisées pour acquérir rapidement des compétences élevées. La plus importante, dénommée « unité 8200 », envoie régulièrement une équipe sur le terrain. Elle traite le renseignement d'origine électromagnétique et le décryptage de code. Des formations sont proposées aux personnels des armées de Terre et de l'Air, de la Marine et des services de renseignement, y compris aux officiers supérieurs. Depuis janvier 2012, le ministère de la Défense dispose d'une administration centrale du cyber pour coordonner les efforts des services de sécurité et appuyer les projets industriels de développement de systèmes avancés. Depuis février 2013, le Centre de cyberdéfense surveille les tentatives d'attaques contre les réseaux militaires. Un document de la Direction des opérations de Tsahal confirme que la doctrine officielle en la matière repose sur le renseignement, la défense et l'attaque. Mais les autorités israéliennes ne reconnaissent pas leur participation à l'élaboration des virus informatiques Flame ou Stuxnet, qui a perturbé le fonctionnement des centrifugeuses nucléaires iraniennes. La stratégie de « dissuasion cybernétique » d'Israël rappelle celle de sa dissuasion nucléaire. Selon Olivier Danino, Israël maintient ainsi une pression sur l'Iran et les pays qui négocient avec lui, en affirmant, de manière détournée, qu'il dispose d'un éventail de moyens, dont le cyber, pour mener avec succès une opération militaire contre les installations nucléaires iraniennes. De son côté, **l'Iran** tente de rattraper son retard en matière de cyber. Il construit son propre « internet national », qui devrait couvrir tout son territoire d'ici à 2015 Depuis 2011, une « cyber police » est chargée de lutter contre la criminalité sur internet et surveiller les réseaux sociaux… pour protéger les Iraniens des logiciels malicieux qui s'y trouvent ! Depuis les ravages du virus Stuxnet, le « Commandement de la défense cyber » s'occupe de la sécurité des infrastructures nationales. En matière d'offensive informatique contre les pays hostiles, l'Iran préfère passer par des entités qui ne lui sont pas rattachées officiellement, afin de nier toute responsabilité en cas d'incidents. Ce fut le cas lors des attaques contre les installations saoudiennes d'hydrocarbures d'Aramco.

En revanche, le groupe « Iran Cyber Army », composé d'informaticiens civils et de hackers (pirates informatiques), est soutenu par l'organisation paramilitaire des Gardiens de la révolution. Un collectif de hackers dénommé « Cyber Hezbollah » tente de mobiliser les partisans du régime iranien pour déclencher le djihad (guerre sainte) dans le cyberspace. Israël, l'Arabie Saoudite, le Qatar et les États-Unis accusent régulièrement l'Iran d'être à l'origine d'attaques informatiques. Depuis le début de la guerre civile en mars 2011, **la Syrie** démontre son savoir-faire dans le cyber. Le régime soutient des mouvements de hackers qui agissent dans son intérêt sans être rattachés à l'État. Ce dernier contrôle totalement l'accès à internet. L'Agence nationale pour la sécurité des réseaux développe les capacités défensives : détection des menaces et réponses aux attaques quotidiennes. La coopération avec l'Iran permet à la Syrie de profiter des progrès que ses spécialistes ont réalisés dans ce domaine.

Acteurs non-étatiques. Les acteurs non-étatiques utilisent beaucoup les réseaux sociaux (Facebook et Google Earth) pour récolter des renseignements. L'organisation terroriste Al-Qaïda et les mouvements politico-militaires Hezbollah (Liban) et Hamas (Bande de Gaza) se servent aussi du cyberespace à des fins de communication, propagande, recrutement et entraînement de partisans, financement d'opérations, explique Olivier Danino. Ainsi, **Al-Qaïda** a appelé à attaquer les systèmes d'information du réseau électrique des Etats-Unis, identifiés comme vulnérables. Le **Hezbollah**, d'obédience chiite, bénéficie du soutien de l'Iran en matière de cyber. Dès novembre 2004, il est parvenu à envoyer un drone de fabrication iranienne en reconnaissance au-dessus du territoire israélien. Pour le **Hamas,** le djihad électronique constitue un nouveau champ de résistance contre Israël. Selon Tsahal, ses hackers, formés par des techniciens iraniens, seront bientôt capables de piloter des drones et d'analyser leurs images. Enfin, de nouveaux groupes de hackers se font connaître lors d'une seule opération puis disparaissent complètement du cyberespace.

Virus informatiques sophistiqués. Olivier Danino classent les virus utilisés au Moyen-Orient selon leur finalité principale : Flame, Gauss, MiniFlame, Duqu et Madhi pour le renseignement ; Stuxnet, Gauss, Wiper et Shamoon pour le sabotage. Le Madhi, d'origine iranienne, a été utilisé contre Israël et en Afghanistan. Il collecte aussi des informations sur des organismes et des personnes en Iran ayant des liens avec les États-Unis. Le Shamoon a touché l'Iran et l'Arabie Saoudite. La prolifération de tous ces virus implique un transfert de

compétences et de matériels d'un État à un autre ou d'un État à un groupe non-étatique. Les effets psychologique et moral du cyber modifient les rapports de puissance au Moyen-Orient, conclut Olivier Danino.

Loïc Salmon

Renseignement : pouvoir et ambiguïté des « SR » des pays arabes

Cyberspace : de la tension à la confrontation ou à la coopération

Les sociétés de sécurité des systèmes d'information Kaspersky (Russie) et Seculert (Israël) ont détecté 3.334 incidents dus aux virus Duqu, Flame, Gauss, MiniFlame et Mahdi dans les pays du Moyen-Orient entre 2009 et 2013. La répartition est la suivante : Liban, 1688 ; Israël, 586 ; Territoires palestiniens, 318 ; Syrie, 34 ; Jordanie, 7 ; Turquie, 3 ; Iran, 598 ; Irak, 6 ; Arabie Saoudite, 20 ; Émirats arabes unis, 19 ; Qatar, 6 ; Bahreïn, 2 ; Koweït, 1 ; Soudan, 37 ; Égypte, 9.