L'utilisation stratégique du cyber au Moyen-Orient

Le cyber fait partie de la panoplie des moyens mobilisés par les Etats du Moyen-Orient pour défendre et protéger leurs intérêts. Toutefois, les pays de la région n'ont pas tous les mêmes capacités cybernétiques ni la même stratégie dans ce domaine. Le gouvernement de Benjamin Netanyahou, par exemple, a fait du cyber une priorité stratégique et a mobilisé d'importantes sommes pour développer les capacités défensive et offensive d'Israël. Les Israéliens ont également engagé plusieurs projets pour sécuriser leurs infrastructures civiles et militaires et pour former les étudiants et les soldats aux enjeux du cyber.

Israël n'est pas le seul Etat du Moyen-Orient à s'investir autant dans le domaine cybernétique. Depuis la découverte de *Stuxnet*, l'Iran a effectivement engagé d'importants moyens financiers pour combler son retard dans ce secteur[1].Téhéran a ainsi mis en place plusieurs infrastructures civiles pour traiter des questions cybernétiques et les Gardiens de la révolution ont créé au sein des Basij le Conseil du cyberespace, une unité cybernétique spécialisée. Du point de vue offensif, l'Iran a adopté une approche indirecte et asymétrique dans le sens où le pouvoir soutient des groupes non-étatiques qui agissent dans son intérêt. La Syrie a d'ailleurs choisi de suivre la même stratégie que son allié iranien avec cependant des moyens moins importants.

Les Etats de la péninsule arabique sont clairement moins avancés qu'Israël ou l'Iran. Ils ont toutefois pris plusieurs mesures pour améliorer la protection de leurs infrastructures critiques depuis la découverte de *Stuxnet* et surtout depuis l'attaque contre les installations d'hydrocarbure en Arabie Saoudite et au Qatar. Les efforts des pays de la péninsule se portent principalement sur l'achat d'outils informatiques leur permettant d'assurer une meilleure sécurité de leurs systèmes d'information et sur la création de CERTs qui occupent une position centrale dans leur organisation défensive. Ce n'est d'ailleurs pas un hasard si le CERT d'Oman accueille en son sein un Centre régional de cyber sécurité. Cette structure, créée en mars 2013, est destinée uniquement aux pays arabes.

Les Etats ne sont pas l'unique acteur du cyberespace moyen-oriental. Il existe effectivement de nombreux groupes non-étatiques au Moyen-Orient. La grande majorité d'entre eux prennent part aux tensions de la région en piratant des sites Internet ou en organisant des opérations cybernétiques massives. Ces attaques restent néanmoins de faible intensité dans le sens où elles ne remettent en cause ni la sécurité des structures visées, ni celle des Etats touchés. D'autres mouvements plus structurés, comme le Hamas, le Hezbollah ou Al-Qaïda, tentent eux de dépasser ces simples compétences en acquérant de réelles capacités cybernétiques offensives. Le Hezbollah se distingue des deux autres mouvements. Le Parti de Dieu, avec l'aide de l'Iran, dispose en effet d'un savoir-faire qui a surpris les Israéliens lors de la guerre de l'été 2006.

[1] *Stuxnet* est le ver informatique qui a endommagé plusieurs installations nucléaires iraniennes.

Par contre, Al-Qaïda, le Hamas et le Hezbollah ont la même utilisation du cyber pour au moins cinq domaines essentiels liés à leur activité : le recrutement et l'entraînement de leurs effectifs, le financement de leur organisation, la propagande, la communication et le renseignement. Le cyber se greffe en fait à d'anciennes pratiques en permettant toutefois de rendre celles-ci plus performantes. C'est une remarque qui est également valable pour les Etats qui organisaient des opérations de renseignement et de sabotage bien avant de disposer de moyens cybernétiques. Néanmoins, les Etats sont les seuls à posséder les fonds et les effectifs nécessaires à l'élaboration de virus sophistiqués. Au Moyen-Orient, les exemples connus se divisent principalement en deux groupes : les malwares qui visent à recueillir des informations, à l'instar de *Flame* ou *Gauss*, et ceux qui ont un potentiel destructeur comme *Stuxnet*, *Shamoon* ou *Wiper*.

Les experts techniques de la société de sécurité informatique russe Kaspersky et ceux de la compagnie israélienne Seculert ont établi que *Stuxnet* et *Duqu* ainsi que *Flame*, *MiniFlame* et *Gauss* découlaient non seulement des mêmes équipes mais qu'ils avaient été conçus dans le cadre du même projet. Or, même si ces virus ont surtout touché Israël, le Liban et l'Iran, plusieurs éléments permettent de supposer que la République islamique est la cible principale de ces attaques.

L'objectif des malwares découverts au Moyen-Orient porte à débat. Certains d'entre eux apparaissent toutefois comme un recours à une opération militaire d'envergure et un moyen de gagner du temps pour laisser la diplomatie faire son chemin, à l'instar de *Stuxnet*, alors que d'autres cherchent plutôt à exercer une pression sur l'Etat visé, et peuvent même parfois être assimilés à des mesures de rétorsion, comme *Shamoon* ou *Wiper*[2]. En ce qui concerne ces deux derniers virus, Kaspersky et Seculert ont trouvé des éléments établissant un lien entre eux et permettant ainsi d'affirmer que les concepteurs de *Shamoon* se sont très probablement inspirés de *Wiper*. Ce qui pose la question de la « prolifération cybernétique » c'est-à-dire de la possibilité pour un Etat de s'inspirer d'un virus dont il a été victime afin d'en mettre au point un autre.

Un deuxième élément attire notre attention. Les compétences acquises par le Hezbollah grâce à l'Iran illustrent la possibilité pour un groupe non-étatique de se doter de capacités cybernétiques par l'intermédiaire d'un Etat et pose donc la question du transfert de ces outils vers un mouvement controversé. Si l'Union européenne ne considère effectivement pas le Hezbollah comme un groupe terroriste, ce n'est pas le cas par exemple des Etats-Unis et du Bahreïn, qui est devenu en avril 2013 le premier Etat arabe à placer le mouvement chiite sur sa liste noire. Toutefois, la possibilité que le cyber soit utilisé à des fins de terrorisme est considérée par les experts comme peu probable. Néanmoins, plusieurs groupes s'intéressent à ce domaine et l'appel lancé par Al-Qaïda en 2012 pour qu'une attaque cybernétique d'envergure soit menée contre les infrastructures critiques des Etats-Unis, et notamment contre le réseau électrique américain, démontre que les failles sont justement repérées et qu'il ne manque à ces mouvements que la capacité d'action.

[2] *Shamoon* est le virus informatique qui a touché les installations d'hydrocarbure d'Arabie saoudite et du Qatar, alors que *Wiper* est celui qui a attaqué les mêmes infrastructures mais en Iran.