L'UTILISATION STRATEGIQUE DU CYBER AU MOYEN-ORIENT

Olivier Danino

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à monsieur **Olivier Danino** cette consultance sur l'utilisation stratégique du cyberespace au Moyen-Orient, sous le numéro de marché 1504119642.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants

Délégation aux Affaires Stratégiques

Sous-direction Politique et Prospective de Défense

14 rue St Dominique

75700 PARIS SP 07

SOMMAIRE

INTRODUCTION

Le Moyen-Orient représente l'un des espaces les plus conflictuels au monde[1]. Les enjeux y sont aussi bien stratégiques, énergétiques, religieux que politiques. En effet, le Moyen-Orient est non seulement au carrefour de trois continents (Europe, Asie, Afrique) mais c'est également le lieu de passage des principaux flux de marchandises maritimes à travers le canal de Suez et les détroits d'Ormuz et de Bab-al-Mandeb. Cet ensemble géographique constitue par ailleurs la première réserve d'hydrocarbures au monde, source de tensions entre certains pays et notamment entre Israël et le Liban suite aux découvertes de gaz en Méditerranée. D'un point de vue religieux, les rivalités au sein des Etats, ou entre les Etats, ne peuvent se résumer à la simple opposition entre chiites et sunnites, surtout que plusieurs courants de l'islam s'affrontent au Moyen-Orient et que la religion musulmane n'est pas la seule concernée. Des tensions existent aussi entre les trois religions monothéistes.

Enfin, l'un des éléments majeurs caractérisant cette région touche aux conflits de territoire. Les litiges frontaliers sont effectivement nombreux. Celui entre Israël et les Palestiniens monopolise l'attention mais il n'est pas le seul. L'Iran et les Emirats arabes unis, l'Arabie Saoudite et le Yémen ou Israël et la Syrie sont autant d'exemples de disputes territoriales pour lesquelles aucune solution n'a encore été trouvée. Ces rivalités ne s'expriment pas uniquement entre Etats dans la mesure où des groupes non-étatiques, comme le Hezbollah libanais ou le Mouvement de la résistance islamique palestinien (plus connu sous le nom de Hamas), y prennent également part.

Le Moyen-Orient est aussi un lieu où les alliances se nouent et se dénouent comme l'illustre la dégradation progressive, au cours des années 1980 et 1990, des relations étroites qui liaient Israël et l'Iran[2]. Notons d'ailleurs que depuis le déclanchement des soulèvements populaires dans le monde arabe, qui ont débuté à la fin de l'année 2010, le climat est propice à un bousculement des alliances régionales et à une évolution des relations entre les différents acteurs de la région. Le Hamas s'est ainsi dissocié de son allié syrien, ce qui a provoqué dans le même temps un refroidissement de ses relations avec l'Iran et un réchauffement de celles avec l'Egypte et les Etats de la Péninsule arabique. L'Egypte, pour sa part, recevait le 5 février 2013 le président Ahmadinejad alors qu'aucun haut représentant iranien ne s'était rendu dans ce pays depuis la révolution islamique de 1979. Cette visite ne signifie pas que le fossé qui existe entre ces deux nations est désormais comblé mais elle marque la reprise d'un dialogue inimaginable sous l'ère Moubarak.

Toutefois, certaines tensions qui existaient entre les différents acteurs de la région avant le déclanchement de ces soulèvements populaires sont exacerbées par ces évènements. Le Yémen accuse ainsi l'Iran de livrer des armes aux mouvements d'opposition alors que le pouvoir syrien profère le même type d'accusations à l'encontre de l'Arabie Saoudite et du Qatar. Le risque d'une

[1] La notion de Moyen-Orient, qui est d'origine anglo-saxonne, comprend une zone géographique étendue, qui peut plus ou moins varier selon les auteurs, alors que l'expression de Proche-Orient, qui regroupe l'Egypte, la Syrie, le Liban, l'Irak, la Jordanie, Israël et les territoires palestiniens, est plus restrictive. Cette étude concerne donc les pays du Proche-Orient, ceux de la Péninsule arabique et l'Iran.

[2] Sur les relations israélo-iraniennes lire le rapport particulièrement intéressant de Dalia Dassa Kaye, Alireza Nader, Parisa Roshan, « Israel and Iran, a dangerous rivalry », The RAND Corporation, 2011, 118 p.

contagion de ces crises se voit donc accru par la situation actuelle. C'est notamment le cas en Syrie, où le contexte de guerre civile contient un fort potentiel d'embrasement régional. Les incidents frontaliers se sont d'ailleurs multipliés avec la Turquie et avec Israël et le bombardement par l'aviation israélienne d'un site proche de Damas, en janvier 2013, illustre clairement le risque d'une contagion du conflit. Le même type de problématique se pose dans la Péninsule du Sinaï dans la mesure où l'instabilité qui règne dans ce secteur trouble la relation entre l'Egypte et Israël. Si les opérations armées en provenance du territoire égyptien devaient s'accroître et gagner en intensité, le risque d'un affrontement plus étendu ne serait effectivement pas à minimiser.

Dans ce climat conflictuel, les Etats du Moyen-Orient, à l'instar de certains groupes non-étatiques, utilisent donc tous les moyens à leur disposition pour défendre et protéger leurs intérêts. Le cyber apparait comme un outil stratégique particulièrement utile étant donné la panoplie d'actions qu'il permet de mener en matière de renseignement, de sabotage et d'opérations militaires mais aussi en termes de communication, d'information et d'attaques, en sachant que celles-ci sont non seulement difficilement détectables et repérables mais aussi parfois très peu coûteuses. Tous les acteurs de la région n'ont cependant pas les mêmes capacités ni la même perception à propos de l'importance stratégique du cyber. En effet, alors que pour certains le domaine cybernétique est une priorité nationale, pour d'autres l'intérêt qu'ils portent à ce sujet ne se résume parfois qu'à la question du contrôle de l'Internet ; quand il n'est pas abordé que sous le seul angle de la criminalité.

La plupart des analyses sur le cyber au Moyen-Orient sont consacrées à un évènement précis. Cette région est effectivement très rarement étudiée dans sa globalité. C'est d'ailleurs ce qui fait l'intérêt de notre démarche et en même temps sa difficulté étant donné que la conséquence directe de cette situation est un éparpillement des sources disponibles et une fragmentation des données par pays. Cette étude se fonde donc sur des informations variées, comme des rapports accessibles en ligne émanant de centres de recherche universitaires et privés, d'organisations internationales et d'Etats, ou encore des ouvrages sur le cyber et d'autres documents plus diversifiés. Les analyses réalisées par des entreprises de sécurité informatique à propos des virus découverts au cours de ces deux dernières années entrent par exemple dans cette dernière catégorie. L'étude que nous proposons repose aussi sur des rencontres avec des experts français et étrangers, sur des conférences et des colloques qui se sont déroulés en France et dans d'autres pays et sur un corpus de documents accessibles en français, en anglais et en hébreu.

Il faut toutefois souligner que le cyber est encore un domaine en maturation. Sans compter que la définition même du mot « cyber », et de ses dérivés, varie selon les experts et les Etats. Les Russes parlent par exemple d'*information technologies* ou d'*information terrorism* là où d'autres évoquent le cyber ou le cyberterrorisme[3]. Par ailleurs, ce n'est pas parce que le même terme est utilisé que la réalité mise derrière est identique. La notion de cyberespace change ainsi d'un pays à l'autre. Pour le Département de Défense américain, le cyberespace est « *a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors*

[3] Alexander S. Adjemov et al., « International Information Security : Problems and Decisions », éd. Komov SA, Moscou, 2011.

and controllers »[4] alors que pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le cyberespace est « un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques »[5].

Dans le cadre de notre propos, il convient surtout de retenir ce que Jean-Loup Samaan appelle les trois strates constitutives du cyberespace :

> « Les experts en sécurité des réseaux reconnaissent trois strates constitutives du cyberespace : la strate physique, la strate syntaxique et la strate sémantique. La strate physique se compose des infrastructures, des câbles, des routeurs et commutateurs : il s'agit de la face la plus concrète du cyberespace. La strate syntaxique met en liaison les deux autres strates en formatant les informations contenues dans le cyberespace, en leur conférant des standards, des protocoles – tel le TCP/IP sur lequel repose Internet. Enfin, la strate sémantique désigne les données brutes véhiculées par le cyberespace et exploitées par les humains ou les machines. Ces informations peuvent aller du simple courriel reçu jusqu'aux images de reconnaissance transmises par un drone aérien à sa station de contrôle en Irak »[6].

Une attaque contre le cyberespace d'un Etat peut donc viser l'une de ces trois strates. Elle peut être menée par des moyens conventionnels comme par des moyens cybernétiques. Le but de notre étude est de mieux saisir comment les différents acteurs du Moyen-Orient appréhendent le cyberespace et comment, dans une zone géographique si conflictuelle, celui-ci est mis à profit d'un point de vue stratégique. Nous nous interrogerons également sur l'existence éventuelle de partenariats entre les Etats, et entre ces-derniers et les groupes non-étatiques de la région. Il s'agit, en d'autres termes, de comprendre la manière dont chacun des acteurs aborde le domaine cybernétique et l'impact qu'a le cyber sur les rapports de forces qui s'expriment au Moyen-Orient.

Il est donc essentiel de dresser une typologie de ces acteurs, de définir la place que le cyber occupe dans leur stratégie, tout en soulignant que l'intérêt pour ce domaine n'émane pas seulement des Etats mais aussi de groupes non-étatiques qui sont particulièrement nombreux au Moyen-Orient. Il est également nécessaire de s'arrêter sur les alliances nouées à l'échelle régionale et internationale afin de mieux comprendre les forces en présence.

Nous analyserons ensuite les tensions du Moyen-Orient sous l'angle du cyber. Le cyberespace est un champ de bataille qui gagne en importance d'année en année et qui fait partie intégrante des conflits actuels et futurs de la région. C'est pourquoi tous les acteurs cherchent à développer des mécanismes de défense pour faire face à la menace et, pour certains, à acquérir leurs propres capacités offensives. Nous évoquerons donc les différents emplois du cyber, la nature des attaques menées et plus largement des exemples de conflictualité dans le cyberespace au Moyen-Orient.

---

[4] Deparment of Defense, « Dictionary of Military and Associated Terms », 15 décembre 2012, p. 74.

[5] Agence nationale de la sécurité des systèmes d'information, « Défense et sécurité des systèmes d'information, stratégie de la France », février 2011, p. 21.

[6] Jean Loup Samaan, « Mythes et réalités des cyberguerres », *Politique étrangère*, IFRI, n° 4, 2008, p. 830.

Partie 1 : Les acteurs du cyberespace

Chapitre 1 : Le poids prépondérant des Etats

Les Etats sont les acteurs principaux du cyberespace au Moyen-Orient pour la simple raison que la maîtrise du domaine cybernétique nécessite non seulement un savoir-faire technique, des infrastructures adéquates et des hommes ayant les compétences nécessaires. Par ailleurs, le développement de certaines capacités défensive et offensive demande des fonds importants qui ne sont pas à la portée de groupes non-étatiques. Il est donc possible d'établir une typologie des Etats de la région, sur la base de ces critères, ce qui permettra dans le même temps d'aborder les stratégies nationales de chacun d'entre eux.

1) Israël, leader régional

Le cyber fait l'objet en Israël d'une attention particulière depuis plusieurs années. L'une des premières initiatives remonte ainsi à 1997 avec la mise en place de *Tehila*[7]. C'est cependant depuis l'accession au pouvoir de Benjamin Netanyahou, en 2009, que les initiatives dans ce domaine se sont multipliées. L'administration Netanyahou considère effectivement le cyber comme une priorité nationale et stratégique. Le Premier ministre israélien souhaite faire de son pays un leader mondial en la matière et a donc décidé de mobiliser des sommes importantes pour y parvenir.

L'intérêt porté au départ par Israël à la protection des systèmes d'information de l'armée a créé un déséquilibre avec ceux du civil. L'un des objectifs aujourd'hui des autorités israéliennes est de combler ce fossé. Benjamin Netanyahou a donc mis en place une commission, composée de 8 experts et dirigée par le professeur Isaac Ben Israël, pour réfléchir à la protection des infrastructures civiles du pays[8]. C'est sous l'impulsion de cette commission que s'est créée en juillet 2011 une institution centrale nommée l'*Israel National Cyber Bureau* (INCB) dirigée par le Dr Evyatar Mataniah et placée sous l'autorité directe du Premier ministre. L'INCB coordonne l'ensemble de l'effort national dans le champ du cyber. Il doit faciliter l'émergence d'une réglementation nationale, collaborer avec les organisations internationales et celles des pays alliés, soutenir l'industrie cyber en Israël et promouvoir la coopération dans ce secteur.

Le gouvernement israélien a mis en place une stratégie qui se décline en quatre points largement complémentaires : la sensibilisation de la population aux enjeux du cyber et à « l'hygiène informatique », l'éducation des jeunes, la recherche scientifique et universitaire et la création d'un socle industriel solide en sécurité des systèmes d'information (SSI). Israël entend effectivement

[7] Tehila est l'infrastructure gouvernementale en charge du secteur de l'Internet dont le but principal est de s'assurer que les institutions gouvernementales et les ministères utilisent Internet en toute sécurité. Pour en savoir plus voir le site officiel : http://147.237.72.58/Tehila1/english_site

[8] Le professeur Ben Israël occupe une place essentielle en raison des nombreuses fonctions qu'il occupe. Spécialiste du renseignement, expert en système balistique, directeur actuel de l'*Israel Aerospace Industries* et du département qui s'occupe du cyber à l'université de Tel-Aviv, il est également un haut officier de l'armée puisqu'il a quitté Tsahal avec le rang de Général de division.

renforcer ses industries spécialisées en SSI à l'instar d'*Elbit Systems* et d'*Elta Systems*, une branche d'*Israel Aerospace Industries*. Ces deux entreprises envisagent d'ailleurs de participer à un consortium de compagnies spécialisées en SSI, avec notamment *Nice* et *Verint*, afin de coordonner leurs efforts et mettre en commun les fonds alloués par l'Etat pour soutenir la R&D. Le gouvernement israélien a en effet décidé d'attribuer près d'un demi-milliard de shekels (soit près de 125 millions de dollars) à ce secteur d'activité qui est considéré par les responsables politiques comme un moteur de croissance économique.

L'éducation des jeunes bénéficie au sein de cette stratégie d'un intérêt particulier. Il s'agit non seulement d'assurer aux entreprises de SSI un réservoir de personnes compétentes mais aussi de former les moins de 18 ans afin qu'ils puissent intégrer avec un minimum de connaissances en main les unités de Tsahal spécialisées dans le cyber. C'est pourquoi, l'armée israélienne a engagé des fonds pour encourager la formation de la jeunesse aux techniques et problématiques cybernétiques. Près de 50 écoles dans tout le pays sont concernées par cette mesure entrée en vigueur pour la rentrée scolaire 2012-2013 en sachant que les jeunes de 14-15 ans pouvaient déjà prendre des cours d'informatique, et même de programmation, et incorporer ces matières dans leurs options du baccalauréat. Depuis décembre 2012, le gouvernement israélien a également lancé un programme national, intitulé en anglais « *cyberwarfare program* », en collaboration avec l'INCB, Tsahal, les services de sécurité de l'Etat, la Fondation Rashi et le ministère de l'Education. Axé sur la formation et le développement de l'expertise dans le domaine cybernétique, ce programme est destiné aux jeunes de 16-18 ans[9].

C'est donc en toute logique, et pour assurer la continuité des efforts portés sur la formation des adolescents israéliens, que l'INCB et le Ministère de la Science et de la Technologie ont décidé d'injecter près de 50 millions de shekels (près de 13 millions de dollars) dans des bourses d'études et de recherche. Plusieurs universités en Israël proposent d'ailleurs des diplômes liés au cyber et pas uniquement dans des matières techniques. Des étudiants travaillent par exemple sur la psychologie des hackers à l'université de Tel-Aviv. L'effort est donc global. La force d'Israël réside dans le fait que la formation commence très tôt et qu'elle se poursuit, pour ceux qui le souhaitent, lors de leur service militaire. Ils arrivent donc à l'université avec des connaissances techniques et pratiques de haut niveau leur donnant la possibilité par la suite de trouver un poste dans le secteur privé ou public.

La conscription joue ici un rôle moteur puisque les jeunes Israéliens se retrouvent dans des unités spécialisées qui sont confrontées tous les jours à des situations cybernétiques particulières leur permettant d'acquérir rapidement des compétences très poussées. La plus connue et la plus importante en nombre de personnes est l'unité 8200[10]. Sa spécialité est le renseignement d'origine électromagnétique et le décryptage de code. Elle a plusieurs services sous sa direction et notamment l'unité *Hatzav*, qui collecte de l'information en *open-source*. L'unité 8200 est particulièrement performante en cryptographie et dispose également d'une unité d'élite qui est projetée régulièrement sur le terrain. L'unité 8200 n'est évidemment pas la seule au sein de l'armée à s'occuper de cyber. La

[9] Pour en savoir plus voir http://embassies.gov.il/UnGeneva/NewsAndEvents/Pages/Opening-national-youth-cyberwarfare-program.aspx

[10] *Yehida Shmoné Matayim* en hébreu.

Direction des services informatiques, par exemple, est en charge des communications et des transmissions au sein de Tsahal. Elle regroupe notamment le *C4I Corps*, une unité opérationnelle (*hayel Ahafala*) et l'unité des télécommunications et des technologies de l'information, plus connue sous le nom de *Lotem*. Cette unité est elle-même divisée en plusieurs sous-groupes[11]. Il serait inutile d'entrer dans le détail de l'organisation militaire israélienne en charge du cyber. Retenons seulement que Tsahal possède un savoir-faire technique, aussi bien dans le domaine défensif qu'offensif, des compétences humaines et une infrastructure structurée qui lui donnent une véritable avance par rapport aux armées des autres Etats de la région.

Néanmoins, des carences persistent. Le réservoir humain reste par exemple trop peu suffisant par rapport aux besoins croissants de l'armée. C'est pourquoi Tsahal multiplie les formations pour ses soldats. Les hommes et femmes qui participent à ces cours sont par la suite envoyés dans l'armée de l'air, de terre, la marine et dans les différentes branches du renseignement. Cet effort a permis à Israël d'augmenter considérablement, et en un temps réduit, le nombre de militaires spécialisés dans le domaine cybernétique. Par contre, les soldats déjà en poste, et notamment ceux de carrières, ne sont pas tous sensibilisés aux enjeux du cyber. C'est pour cette raison que le *C4I Corps* a lancé en juin 2012 un vaste programme pour enseigner aux officiers supérieurs la manière dont ce domaine affecte les opérations sur le terrain et les conflits dans lesquels l'armée est engagée.

Les initiatives israéliennes ne se résument pas à la dimension humaine du cyber. Elles concernent aussi l'organisation globale de la structure militaire. Le ministère de la Défense s'est ainsi doté depuis janvier 2012 d'une administration centrale en charge du cyber dont la mission est de coordonner les efforts des services de sécurité israéliens et d'appuyer les industries de défense dans leur projet de développement de systèmes cybernétiques avancés. L'armée, de son côté, a mis en place depuis février 2013 un centre de cyberdéfense pour surveiller les tentatives d'attaques sur les réseaux militaires[12]. Composé pour le moment d'une vingtaine de soldats, cette structure est opérationnelle 24h sur 24 et 7 jours sur 7. Le nombre de soldats qui la compose est appelé à augmenter au courant de l'année 2013. Ce centre de cyberdéfense travaille étroitement avec *Tehila* et les services intérieurs de sécurité, le Shin Beth, qui assurent la sécurité des infrastructures critiques du pays (énergie, marchés financiers, réseaux de communication et secteur des transports).

L'armée israélienne ne travaille pas que sur l'aspect défensif du cyber. Comme l'a reconnu en juin 2012 le ministre de la Défense, Ehud Barak, si Israël considère cette dimension comme la plus importante et la plus complexe, Tsahal développe également des moyens offensifs car l'armée ne

[11] Pour plus de détails voir le site officiel de Tsahal qui détaille l'organisation de l'armée et où l'on peut notamment trouver des informations sur le *C4I Corps*.

[12] Yaacov Lappin, « IDF Cyber Center Control Center goes on line », Jerusalem Post, 13 février 2013, http://www.jpost.com/Defense/Article.aspx?ID=303089. Un mois après la création de centre de cyberdéfense, l'Administration pour le développement des armes et de l'infrastructure technologique, qui coordonne l'action entre le ministère de la Défense, l'armée, les industries militaires, l'*Israel Aerospace Industries*, l'Agence spatiale israélienne et l'Institut de recherche biologique, a lancé un directoire cybernétique pour centraliser les efforts menés par ces différents organismes dans le domaine cybernétique. Voir Or Heller, « New Cyber Directorate in Mafat », 12 mars 2013, http://www.israeldefense.com/?CategoryID=512&ArticleID=2012

peut pas se contenter de rester dans un mode passif en ne réagissant qu'aux attaques[13]. C'est la première fois qu'un aussi haut responsable politique reconnaît publiquement la dimension offensive de la stratégie cybernétique d'Israël. Ehud Barak confirme ainsi une note écrite quelques jours plus tôt par Rotem Pesso, intitulée « *IDF in cyber space: Intelligence gathering and clandestine operations* », et publiée sur le site Internet de Tsahal[14]. Ce texte, très court, évoque les principaux éléments qui guident l'action de l'armée israélienne dans le cyberespace, en se référant à un document de la Direction des Opérations, et confirme que la doctrine cybernétique d'Israël est constituée du triptyque renseignement, défense et attaque. En le lisant, on ne peut s'empêcher de penser au raid israélien mené en 2007 contre le réacteur nucléaire syrien et aux opérations cybernétiques lancées contre le programme nucléaire iranien et notamment au ver informatique *Stuxnet*[15]. Surtout que la publication de cette note intervient à un moment particulier puisque quelques jours auparavant les laboratoires Kaspersky révélaient la découverte de *Flame*, un malware très puissant, et particulièrement actif au Moyen-Orient, dont la principale caractéristique est de voler de l'information (e-mails, capture d'écran, enregistrement des touches du clavier ou enregistrement de conversations audio par exemple).

Néanmoins, si les autorités israéliennes assument publiquement leurs activités offensives dans le cyberespace, elles ne reconnaissent pas pour autant être à l'origine de virus comme *Flame* ou *Stuxnet*. Cette ambiguïté semble s'inscrire dans une stratégie de « dissuasion cybernétique » qui n'est d'ailleurs pas sans rappeler la doctrine nucléaire israélienne. Israël semble donc être passé à une nouvelle étape dans sa manière d'aborder la question du cyber. Pourquoi le faire à ce moment précis alors que jusque là le silence prévalait ? Parce qu'en le faisant, Israël maintient la pression sur l'Iran et sur les pays qui négocient avec Téhéran puisque c'est une manière détournée d'affirmer qu'Israël dispose d'un éventail large de moyens, dont fait partie le cyber, pour mener à bien une éventuelle opération militaire contre les installations nucléaires iraniennes. Ce choix n'est donc pas anodin. L'Iran, qui a été la cible de plusieurs virus informatiques, a d'ailleurs pris conscience de l'importance stratégique du cyber et a décidé de prendre à bras-le-corps ce problème.

2) L'Iran cherche à rattraper son retard

L'Iran était sensible à la question du cyber bien avant d'être la cible d'attaques sophistiquées. Il ne fait toutefois aucun doute qu'elles ont conduit le pouvoir iranien à une remise en question et à un réajustement de sa stratégie cybernétique. L'Iran a donc décidé de consacrer davantage de moyens

[13] Vita Bekker, Barak admits Israel's cyberwar activity, Financial Times, 6 juin 2012, http://www.ft.com/cms/s/0/43f199f2-afec-11e1-b737-00144feabdc0.html

[14] Voir l'annexe 1 de cette étude (p. 49).

[15] Stuxnet a été découvert à la mi-juin 2010 par VirusBlokAda, une société spécialisée dans la sécurité des systèmes d'information basée en Biélorussie. Stuxnet est un ver informatique, c'est-à-dire un virus qui se propage par les réseaux, qui a infecté des systèmes industriels iraniens et en particulier les centrifugeuses de la centrale nucléaire de Natanz. Stuxnet n'est pas passé par Internet, ce qui laisse croire à une inoculation du ver par un être humain. Pour plus d'informations, voir l'excellent rapport du Congressional Research Service : Paul K. Kerr, John Rollins, Catherine A. Theohary, « The Stuxnet Computer Worm : Harbinger of an Emerging Warfare Capability », CRS report for Congress, 9 décembre 2010, 9 p.

pour combler le retard qui était le sien dans ce domaine. Selon Frank J. Cilluffo, le directeur du *Homeland Security Policy Institute* de l'université George Washington, le gouvernement de Téhéran a ainsi mobilisé un milliard de dollars pour renforcer ses capacités cybernétiques aussi bien du point de vue défensif qu'offensif[16]. Quelle que soit la réalité de ce chiffre, la volonté iranienne de faire du cyber une priorité est bien réelle. Pour l'Iran, le domaine cybernétique constitue effectivement un élément qu'il faut désormais intégrer à toute réflexion stratégique dans la mesure où il modifie non seulement le rapport de force entre les Etats mais qu'il a aussi des conséquences directes sur le déroulement des combats armés. Le commandant des forces anti-aériennes des Gardiens de la révolution, le général Farzad Esmaili, affirmait d'ailleurs en octobre 2012 que les prochaines guerres auxquelles l'Iran devra faire face n'auront rien à voir avec les précédentes[17].

C'est donc dans cette optique que les dirigeants iraniens ont entrepris la construction d'un « Internet national », parallèle à « l'Internet global », auquel la population sera connectée au courant de l'année 2013[18]. L'ensemble du territoire devrait être couvert d'ici à 2015. Pour le moment, seules les institutions gouvernementales fonctionnent sur ce réseau de données. La plupart des experts doutent que la création d'un « Internet national » puisse protéger efficacement l'Iran contre d'éventuels virus informatiques sophistiqués mais le pouvoir iranien considère que la sécurité du pays passe par un Internet entièrement sous contrôle. C'est d'ailleurs pour cette raison que le gouvernement iranien a créé, en janvier 2011, une unité de « cyber police » dont le but précis est de surveiller l'Internet et d'y combattre toute forme de criminalité. En novembre 2011, les policiers de ce groupe ont intégré à leur service des hackers pour pouvoir infiltrer des sites, des comptes e-mails et des forums. De plus, l'Iran a annoncé en janvier 2013 avoir mis en place un logiciel pour aider les autorités à surveiller les réseaux sociaux. La création de ce software est justifiée officiellement par la nécessité de protéger les Iraniens d'éventuels logiciels malicieux qui se trouvent sur ces réseaux.

L'Internet occupe donc une place particulière dans la stratégie iranienne même si les mesures de défense adoptées par l'Iran ne peuvent se résumer à cet aspect. Le pouvoir iranien a effectivement entrepris depuis 2010 une rationalisation de ses infrastructures en charge du cyber à travers la création du *Cyber Defense Command* en novembre 2010 et, en mars 2012, du Conseil Suprême du Cyberespace. Le *Cyber Defense Command* , placé sous l'autorité de l'Organisation de la défense passive iranienne, est en charge de la défense du pays et de la sécurité des infrastructures nationales. Sa création est en grande partie due à la découverte dans les installations nucléaires iraniennes du ver informatique *Stuxnet*. Le Conseil Suprême du Cyberespace fait pour sa part office d'organe central dans le dispositif iranien. C'est lui qui dicte la direction à suivre à l'ensemble des organisations nationales en charge du cyber. Il est d'ailleurs composé des plus hautes autorités du pays. L'une de ses principales missions est de mettre en place un Centre National du Cyberespace qui aura comme responsabilité d'élaborer les réponses adéquates pour l'ensemble des enjeux nationaux et internationaux liés au cyber.

---

[16] « The Iranian Cyber Threat to the United States », témoignage de Frank J. Cilluffo devant le US House of representatives, Committee on Homeland Security,Homeland Security Policy Institute, 26 avril 2012, 9 p.

[17] Fars News Agency, « Iran Boosting Electronic War Capabilities due to Nature of Threats », 1er octobre 2012, http://english.farsnews.com/newstext.php?nn=9106243312

[18] Al Jazeera, « Iran to launch giant domestic intranet », 24 septembre 2012, http://www.aljazeera.com/news/middleeast/2012/09/201292471215311826.html

En ce qui concerne l'aspect offensif, l'Iran a fait le choix de favoriser la confrontation indirecte avec les pays qu'il juge hostiles. Plutôt que l'opposition frontale, le pouvoir iranien préfère passer par l'intermédiaire d'adversaires interposés. L'Iran appuie donc des mouvements qui ne lui sont pas rattachés officiellement mais qui agissent dans son intérêt. Les dirigeants iraniens ont ainsi maintenu dans le domaine cybernétique la stratégie qui est la leur depuis plusieurs années[19]. Un tel choix permettant d'éviter une implication directe de l'Iran et donc la possibilité de nier assez facilement toute responsabilité dans d'éventuels incidents. Ainsi, lorsque les autorités saoudiennes ont accusé l'Iran d'être à l'origine des attaques cybernétiques qui ont visé les installations d'Aramco, les dirigeants iraniens ont déclaré qu'ils n'étaient pas responsables de cette opération revendiquée par un groupe appelé *Cutting Sword Of Justice*. Ce groupe s'est d'ailleurs fait connaître à ce moment-là mais est resté depuis particulièrement discret. Pour les services de sécurité américains, il ne fait aucun doute que *Cutting Sword of Justice* a agi avec le soutien du pouvoir iranien. Les experts techniques considèrent que le virus informatiques utilisé pour cette opération n'a pas pu être conçu par un simple groupe de hackers mais ils n'ont pas pour autant prouvé que l'Iran se trouvait derrière cette attaque.

Le lien avec le pouvoir iranien est par contre plus clair en ce qui concerne d'autres groupes. C'est le cas par exemple de l'*Iran Cyber Army* (ICA) qui est composée de spécialistes informatiques et de hackers professionnels. L'ICA regrouperait plusieurs mouvements de hackers actifs dans le pays depuis plusieurs années[20]. Ce sont tous des civils soutenus directement par les Gardiens de la révolution. Le pouvoir iranien semble également avoir établi une relation privilégiée avec une entreprise privée de sécurité informatique, l'*Ashiyane Security Group*, fondée en 2002 par Behrooz Kamalian. Si *Ashiyane* produit et vend des logiciels SSI, le groupe a aussi revendiqué des opérations de piratage, notamment contre des sites Internet israéliens et américains, qui restent toutefois d'un niveau technique peu élevé. Outre l'ICA et à *Ashiyane*, les autorités iraniennes soutiennent un collectif de hackers, appelée *Cyber Hezbollah*, dont certains des membres ont appuyé le pouvoir iranien lors des évènements de 2009[21]. Le *Cyber Hezbollah* souhaite mobiliser les partisans du régime iranien et faire avancer la réflexion sur les moyens adéquats de mener le jihad dans le cyberespace. Il tient d'ailleurs régulièrement des réunions sur cette thématique à Téhéran. La conférence du 12 juillet 2012, par exemple, était consacrée à la situation en Syrie. Le *Meir Amit Intelligence and Terrorism Information Center*, un centre israélien créé en 2002, décrit ainsi l'action du *Cyber Hezbollah* :

> *« A memorandum of opinion released by the organization shortly after it was established listed its goals and objectives, which include bringing together [iranian] regime supporters who are active in cyberspace, organizing courses and training for the activists, holding meetings to acquaint the activists with tactics of cyber warfare, and mobilizing the activists for online activities »*[22].

[19] Voir François Géré, « Iran, état de crise », Lignes de repères, éd. Karthala, 2010, p. 53.

[20] Khashayar Nouri, « Cyber wars in Iran », Mianeh, 22 juillet 2010, http://mianeh.net/article/cyber-wars-iran

[21] L'Iran connaissait à cette époque une contestation populaire massive en raison des résultats aux élections présidentielles de juin 2009.

[22] Raz Zimmt, « Spotlight on Iran », semaine du 11 au 18 juillet 2012, http://www.terrorism-info.org.il/en/article/20370

Ce collectif de hackers constitue l'un des exemples les plus explicites de la stratégie adoptée par l'Iran. Il ne faut cependant pas confondre le *Cyber Hezbollah* avec le mouvement dirigé par Hassan Nasrallah même si le Hezbollah libanais bénéficie aussi du soutien de son allié iranien en matière de cyber.

Pour coordonner cette stratégie d'affrontement asymétrique dans le cyberespace, l'Iran dispose d'une unité cybernétique au sein des Basij, les Forces de mobilisation de la résistance, une branche des Gardiens de la révolution. Il s'agit du Conseil du cyberespace créé en 2010 par les Basij. Ce conseil travaille donc étroitement avec plusieurs groupes de hackers et mobilise les spécialistes du cyber au sein des Gardiens de la révolution pour former de nouveaux pirates informatiques et les aider à acquérir des compétences de haut niveau. Selon Hussein Hamedani, l'ancien commandant de la province de Téhéran, au moins 1500 individus sont passés jusqu'ici par cette structure[23]. L'un des architectes des activités cybernétiques des forces armées iraniennes est le Dr Hassan Abbassi, un scientifique iranien membre des Gardiens de la révolution et conseillé spécial auprès du président Ahmadinejad.

Au regard de toutes ces initiatives, plusieurs pays accusent régulièrement l'Iran d'être à l'origine d'attaques dont ils sont la cible. L'Arabie Saoudite et le Qatar, par exemple, mais aussi Israël, qui affirme que ses systèmes d'information sont quotidiennement visés par des tentatives d'infiltration iraniennes, et les Etats-Unis qui imputent à Téhéran la responsabilité des attaques cybernétiques ayant touché plusieurs banques américaines entre septembre 2012 et janvier 2013. Les autorités américaines pensent que ces incidents sont une réponse aux sanctions économiques imposées par l'administration Obama à l'Iran en raison de la dimension militaire de son programme nucléaire.

Il y a encore quelques années, aucun expert n'aurait pensé mentionner l'Iran parmi les pays disposant de capacités cybernétiques efficientes. Pourtant, Téhéran a réussi à développer ses moyens défensifs comme offensifs en très peu de temps. Les Iraniens ont non seulement très vite appris mais ils ont montré une capacité d'adaptation surprenante. Nous reviendrons plus tard sur les cas de *Mahdi* et de *Shamoon*, deux virus supposés d'origine iranienne, qui illustrent précisément cet état de fait.

3) Le réveil des autres Etats de la région

Le domaine cybernétique n'a pas toujours été perçu comme une urgence stratégique par les autres pays de la région. En réalité, cette prise de conscience s'est faite progressivement. D'abord due à la multiplication des attaques, plus ou moins virulentes, dont ils ont tous été la cible, c'est la découverte en 2010 du ver informatique *Stuxnet* qui est véritablement à l'origine du « réveil cybernétique » des Etats du Moyen-Orient[24].

Dans la péninsule arabique, la question du cyber a d'abord été abordée sous l'angle de la cybercriminalité. Entendu dans un sens large, qui mélange aussi bien les questions de moralité, de

[23] Hossein Bastani, « Structure of Iran's Cyber Warfare », BBC Persian, en ligne sur http://www.strato-analyse.org/fr/spip.php?article223

[24] Sauf pour Israël comme nous l'avons vu.

sécurité et de politique, ce sujet a fait l'objet très rapidement d'une législation stricte au sein des pays de cette région. Si la cybercriminalité continue d'être une thématique traitée, la péninsule arabique s'intéresse aujourd'hui davantage à la dimension défensive du cyber. Pour répondre à cette problématique, les Etats mettent notamment à profit les relations privilégiées qu'ils entretiennent avec les entreprises américaines de SSI et avec le gouvernement des Etats-Unis, en particulier en matière de défense. Si la vision américaine tend à influencer progressivement l'approche qu'ont ces pays de la question cybernétique, il n'en reste pas moins que chaque gouvernement développe sa propre analyse et prend ses propres mesures.

Néanmoins, la particularité de la péninsule arabique réside dans le fait que la sécurité des systèmes d'information a été confiée dans la plupart des Etats à des CERT (*Computer Emergency Response Team*) et non à des organismes centraux comme c'est le cas en Israël ou en Iran. Ces CERT sont toutefois rattachés à un organisme national qui dépend directement du pouvoir. Ainsi, le CERT du Qatar, appelé QCERT, dépend du Conseil suprême des communications et des technologies de l'information fondé en 2004. Le QCERT travaille en collaboration étroite avec les secteurs publics et privés et c'est en son sein qu'a lieu la réflexion sur la stratégie cybernétique de l'émirat[25]. Au Qatar, le secteur privé est associé activement à l'effort national, surtout depuis l'attaque dont a été victime RasGas, l'entreprise national de gaz liquéfié, au courant de l'été 2012. L'Institut qatari de recherche informatique (QCRI) a d'ailleurs annoncé en mars 2013 qu'il mettait en place un centre d'analyse dont le but est de fournir les outils nécessaires à la protection de l'émirat.

En Arabie Saoudite, le CERT est placé sous l'autorité de la Commission des technologies de la communication et de l'information créée en 2001 par le roi Fahd Ben Abel Aziz Al-Saoud. Si ce CERT dispose de larges prérogatives, il n'en reste pas moins que tous les ministères du royaume ne sont pas encore connectés à lui, limitant par conséquent son action[26]. En 2011, sous l'impulsion d'une résolution adoptée par le ministère des communications et des technologies de l'information, l'Arabie Saoudite a publié un texte intitulé « *Developing National Information Security Strategy for the Kingdom of Saudi Arabia* » [27]. Ce document fixe les objectifs du royaume saoudien en matière cybernétique et propose 9 axes sur lesquels l'Arabie Saoudite doit particulièrement engager ses efforts, parmi lesquels les ressources humaines, la coopération à l'échelle nationale et internationale ou encore la recherche et l'innovation. Ce qui ne veut pas dire que les autorités saoudiennes n'avaient rien fait sur ces sujets auparavant comme l'illustre le centre de recherche créé en 2008 par l'université King Saud et l'entreprise de sécurité informatique Al-Elm.

Cet exemple de coopération entre le secteur universitaire et le milieu industriel n'est pas le seul de la péninsule arabique. Ainsi, aux Emirats arabes unis, l'université Khalifa s'est associée en 2010 à Emiraje Systems pour monter un centre d'excellence, connu sous le nom de *Cyber Operations*

[25] Néanmoins, c'est sur le site du Conseil suprême que l'on peut trouver un document relatif à la stratégie du Qatar en matière de protection de ses infrastructures critiques. Ce document a été publié en janvier 2012, soit quelques mois avant l'attaque dont a été victime l'émirat. Il n'a pas été mis à jour depuis. Intitulé « Controls for the Security of Critical Industrial Automation and Control Systems Guidelines », il est accessible sur http://www.ictqatar.qa/sites/default/files/documents/Controls_English_Version_0.pdf

[26] Pour en savoir plus sur les missions du CERT saoudien, voir son site Internet http://cert.gov.sa/index.php?option=com_content&task=view&id=69&Itemid=116

[27] Le document complet est disponible en ligne. Voir http://www.mcit.gov.sa/NR/rdonlyres/514E7B51-5710-46D9-9EC5-2D78BC2E1219/0/NISS_Draft_7_EN.pdf

Center of Excellence. La différence toutefois avec l'Arabie Saoudite réside dans le fait que ce projet est coordonné avec les forces armées et qu'il est mené en collaboration avec Cassidian, la branche cyber sécurité d'EADS. La création de ce centre d'excellence est un parfait exemple du dynamisme émirati. En effet, depuis quelques années, les Emirats arabes unis multiplient les initiatives dans le domaine cybernétique. Ainsi, en 2008, l'Autorité de régulation des télécommunications mettait en place un CERT dont la mission était de coordonner l'ensemble de la sécurité de l'Etat.

Les attaques menées par des hackers israéliens sur le site Internet de la bourse d'Abou Dhabi, et surtout l'attaque contre les infrastructures critiques de l'Arabie Saoudite et du Qatar à l'été 2012, ont conduit les Emirats arabes unis à compléter ce dispositif. Le gouvernement fédéral a ainsi émis un décret, à la fin de l'année 2012, qui stipule la création de l'Autorité nationale de sécurité électronique (ANSE) placée sous la responsabilité directe du Conseil suprême de la sécurité nationale. Responsable de la mise en œuvre et de l'élaboration de la politique nationale des Emirats arabes unis en matière de SSI, l'ANSE s'occupe également des menaces et des attaques cybernétiques et du renforcement du réseau de communication et d'information émirati. L'ANSE est dirigée par un conseil d'administration, élu par le président du Conseil suprême de la sécurité nationale, pour une période de trois ans.

Les Emirats arabes unis sont donc en avance sur bien de leurs voisins à l'instar du Bahreïn qui n'a mis en place son CERT qu'en Novembre 2012. Le royaume dispose cependant de plusieurs structures, comme l'Organisation centrale de l'informatique (CIO en anglais), qui gère le fonctionnement de l'Internet et de ses données, ou du tout nouveau *Directorate for Combatting Corruption and for Electronic and Economic Security* qui dépend du Ministère de l'Intérieur et dont la mission est la lutte contre la cybercriminalité.

Le Yémen par contre est le moins compétent des Etats de la péninsule arabique. Ne disposant ni d'infrastructures cybernétiques sophistiquées, ni de véritables connaissances dans ce domaine, le pouvoir s'est tourné vers les Etats-Unis pour l'aider à protéger ses systèmes d'information. De ce point de vue, le Yémen se distingue complètement de l'exemple bahreïni ou du cas syrien. En effet, la Syrie fait preuve d'un vrai savoir-faire dans le domaine cybernétique qu'elle démontre tous les jours depuis le soulèvement, en mars 2011, de sa population contre le président Bachar el-Assad. La stratégie offensive du dirigeant syrien s'inspire largement de celle de son allié iranien. Elle consiste effectivement à soutenir des mouvements de hackers qui ne sont pas rattachés officiellement à l'Etat mais qui agissent malgré tout dans son intérêt. De cette manière, Bachar el-Assad dispose de capacités qu'il peut mobiliser à tout moment. L'aspect défensif repose quant à lui sur un contrôle quasi complet de l'accès à Internet par l'Etat et sur les compétences de la *National Agency for Networks Security*, qui a fondé un CERT appelé l'*Information Security Center* dont la mission est justement de développer les capacités défensives de la Syrie et de proposer des solutions pour détecter les menaces et répondre aux attaques. Le fait d'être confrontés quotidiennement à des attaques a été pour les dirigeants syriens l'occasion d'améliorer leur approche du sujet et d'adapter leur stratégie en conséquent. La coopération avec l'Iran est également un facteur important puisque la Syrie a pu bénéficier ainsi des progrès de Téhéran. Ce qui pose la question des alliances régionales et des collaborations internationales.

4) Les alliances régionales et internationales

Israël, l'Iran, la Syrie, le Liban et tous les Etats de la péninsule arabique sont membres de l'*International Multilateral Partnership Against Cyber Threat* (IMPACT) qui est la branche de l'*International Telecommunication Union* (ITU) en charge de cyber sécurité. L'ITU est un organisme qui dépend des Nations unies. C'est sous son auspice, par exemple, qu'a été organisée la Conférence mondiale des télécommunications internationales qui s'est déroulée à Dubaï du 3 au 14 décembre 2012[28]. L'objectif de l'IMPACT est d'aider les Nations unies à protéger ses infrastructures et de fournir à tous ses membres un accès à une expertise spécialisée et à des ressources pour lutter efficacement contre les menaces cybernétiques. L'IMPACT s'est d'ailleurs associée à l'Autorité des technologies de l'information (ATI) d'Oman pour créer dans ce sultanat un Centre régional de cyber sécurité (CRCS) afin d'aider les pays arabes à sécuriser leurs systèmes d'information économiques et les encourager à mettre en place des centres nationaux en charge du cyber. Le CRCS a également pour responsabilité d'organiser des exercices de simulations régionaux pour permettre à ses membres de faire face à des crises cybernétiques majeures. C'est donc une initiative importante du point de vue du développement des capacités défensives de la région même si on peut se demander dans quelles mesures les Etats participeront à ses activités et quelles seront ses impacts réels sur les compétences des gouvernements arabes ?

Le choix d'Oman pour accueillir cette structure est le fruit des efforts menés par le sultanat dans le domaine cybernétique depuis plusieurs années. L'ATI a ainsi été fondé le 31 mai 2006 afin d'améliorer la connectivité des institutions gouvernementales, de l'économie et des citoyens du sultanat. L'analyse des risques, la sécurité du cyberespace et la protection de l'Internet étant assurées par le CERT d'Oman crée en avril 2010. C'est d'ailleurs en son sein que le Centre régional de cyber sécurité a vu le jour le 4 mars 2013. La création de ce Centre régional au sein d'un CERT n'est pas anodine. Elle découle de la stratégie défensive adoptée par les Etats de la péninsule arabique. Le fait qu'il soit situé dans cette région interroge par ailleurs sur sa possible évolution en structure de défense face à l'Iran ou à Israël qui en sont par définition exclus étant donné que ce centre est destiné uniquement aux pays arabes.

Surtout qu'il existe déjà une organisation internationale qui regroupe les CERT des pays musulmans : l'*Organisation for Islamic Cooperation – Computer Emergency Response Team* (OIC-CERT), créée en juin 2005 par l'Organisation de la coopération islamique (OCI). Sur les 57 membres de l'OCI, seuls 18 en font partie[29]. Parmi ces 18 Etats, plusieurs entretiennent des relations diplomatiques conflictuelles et certains sont même soupçonnés d'avoir mené des attaques cybernétiques contre d'autres. Le meilleur exemple concerne bien entendu l'Iran et l'Arabie Saoudite. Ce contexte de tension et de suspicion n'est pas propice à une coopération constructive et il n'est donc pas étonnant de voir naître un Centre régional de cyber sécurité des pays arabes. Il est

[28] Pour en savoir plus sur cette conférence voir le dossier du site de l'UIT : http://www.itu.int/en/wcit-12/Pages/default.aspx. L'un des sujets abordé lors de cet événement concerne la présence de certains organismes stratégiques sur le territoire américain, comme l'ICANN qui est chargé des noms de domaine. La Russie et les Emirats arabes unis, par exemple, se sont prononcés pour l'internationalisation de ces organismes. Ce point est profondément stratégique dans le sens où la question posée en toile de fond concerne le pouvoir dont disposent les Etats-Unis sur l'Internet et les capacités de ce pays à contrôler le réseau mondial.

[29] Le Maroc, Oman, la Tunisie, la Malaisie, la Syrie, le Pakistan, le Nigéria, la Jordanie, l'Iran, Brunei, l'Arabie Saoudite, l'Egypte, l'Indonésie, la Libye, le Bengladesh, la Turquie, les Emirats arabes unis et le Soudan.

d'ailleurs intéressant de noter que l'OIC-CERT a participé en février 2012 à l'exercice annuel de simulation organisée par son homologue d'Asie pacifique, l'APCERT, mais que sur les 22 pays présents seuls le Pakistan, la Tunisie et l'Egypte représentaient l'OIC-CERT.

Et si les Etats comme l'Arabie Saoudite et les Emirats arabes unis rechignent à participer aux exercices de l'OIC-CERT, d'autres comme le Qatar ne font même pas partie de cette structure. Quant à la Turquie, qui elle en est membre, elle semble préférer se tourner vers l'Organisation du Traité de l'Atlantique Nord (OTAN). Le *Cyber Defense Command*, mis en place au sein des forces armées turques en 2012, opère effectivement en coordination avec le ministère des Transports maritimes et des communications, le Conseil de la recherche scientifique et technologique de Turquie (TUBITAK) et avec l'OTAN aussi bien pour ses missions nationales qu'internationales. Le choix stratégique turc de s'investir davantage avec l'OTAN ne concerne pas que le *Cyber Defense Command*. La Turquie a effectivement fait savoir qu'elle souhaitait intégrer le Centre d'excellence de Tallinn. Si c'était le cas, elle deviendrait le 13^{e} membre après la France à rejoindre cette organisation.

Les pays du Moyen-Orient participent donc à plusieurs collaborations dans le domaine cybernétique qui peuvent s'inscrire dans des structures régionales ou internationales comme dans des partenariats entre Etats. Cette coopération n'est pas que régionale puis qu'Israël et l'Arabie Saoudite travaillent avec les Etats-Unis et l'Iran et la Syrie avec la Russie et la Chine. Néanmoins, l'échelle par excellence reste celle du local. Les projets sont effectivement le plus souvent le fruit de décisions gouvernementales et portent sur des structures étatiques ou en collaboration avec le monde universitaire et l'industrie SSI. Dans une région où les antagonismes sont si forts, il n'est pas surprenant que les choses se passent ainsi. Mais au Moyen-Orient, les Etats ne sont pas les seuls à s'intéresser au cyber. C'est également le cas de mouvements non-étatiques.

Chapitre 2 : Des groupes nombreux et variés

Les Etats ne sont pas les seuls acteurs du cyberespace moyen-oriental. Il existe effectivement de nombreux groupes non-étatiques de nature diverse et aux objectifs variés. Certains font parler d'eux tous les jours étant donné qu'ils mènent régulièrement des attaques. Agissant en fonction de leurs intérêts, ces groupes sont parfois étroitement liés au gouvernement d'un pays. Le cas d'Anonymous est quant à lui intéressant car ce mouvement est particulièrement actif au Moyen-Orient. Toutefois, si le mode opératoire d'Anonymous est similaire à celui des autres hackers de la région, il ne faut pas placer ce collectif à égalité avec les autres groupes de la région. Il reste un acteur mineur au Moyen-Orient. Par contre, d'autres mouvements, comme Al-Qaïda, le Hezbollah ou le Hamas, cherchent à acquérir des capacités de haut niveau qu'ils souhaitent intégrer à leur stratégie et à leurs outils offensifs.

1) Les acteurs non-étatiques et leurs liens avec les Etats du Moyen-Orient

Le Moyen-Orient, comme d'autres régions, pullule de pirates informatiques qui agissent indépendamment de toutes structures. Ils appartiennent le plus souvent à des groupes de hackers qui sont peu organisés, et au sein desquels il n'existe aucune hiérarchie, même si certains peuvent aussi agir seuls, en leur propre nom. La grande majorité d'entre eux justifie leurs actions par un discours politique plus ou moins construit. C'est le cas par exemple du hacker Anonyme 972, qui a rendu public les adresses et mots de passe de messageries d'étudiants saoudiens, et d'un pirate informatique lié au group-xp, du nom d'0xOmar, qui a dévoilé des milliers de numéros de cartes de crédit appartenant à des citoyens israéliens. Ces deux opérations se sont déroulées en janvier 2012.

Il existe également des mouvements comme l'*International Muslim's Cyber Army* ou les *Muslim Liberation Army* qui sont des groupes défendant une idéologie islamiste. Ils prennent aussi bien pour cible des pays musulmans, comme l'Arabie Saoudite, que des Etats jugés hostiles, comme Israël. Pour eux, ces actions s'inscrivent dans un jihad cybernétique. On parle alors de « cyber jihad » ou de « e-jihad ». La seconde conférence du *Cyber Hezbollah*, tenue à Téhéran en septembre 2011, était d'ailleurs consacrée à ce sujet. Intitulé « Clic de résistance », cet évènement portait sur les moyens de mener le jihad dans le cyberespace et sur la manière de mettre en valeur les blogs dédiés à la résistance et aux opérations des différents groupes jihadistes. La principale intervention a été donnée par le Dr Hassan Abbassi, le directeur du Centre des études doctrinales et stratégiques iranien.

Le jihad électronique a aussi été mis en avant par Al-Qaïda dans une vidéo rendue publique par les autorités américaines en 2012. Le mouvement appelait à s'en prendre aux intérêts du gouvernement des Etats-Unis et à attaquer les infrastructures critiques du pays, en particulier les systèmes d'information du réseau électrique qui ont été identifiés à juste titre par Al-Qaïda comme un des points faibles majeurs des Etats-Unis. La vidéo compare cette vulnérabilité aux imperfections de la

sécurité aérienne des Etats-Unis avant les attentats du 11 septembre 2001, faisant ainsi un parallèle entre ces deux types d'attaque[30].

Al-Qaïda n'est pas la seule organisation à avoir appelé au jihad électronique. Le Hamas, par exemple, considère que c'est un nouveau champ de résistance contre Israël. Des personnalités religieuses ont également fait le même type de déclarations, comme Tarek Mohammed Al-Suwaidan, un imam de nationalité koweitienne, qui publiait sur son compte twitter, le 18 janvier 2012, un appel à l'union des hackers arabes pour conduire le « cyber-jihad contre l'ennemi sioniste »[31]. Pour le vice-ministre des Affaires étrangères d'Israël de l'époque, Danny Ayalon, à partir du moment où ces attaques violent la souveraineté de son pays, elles sont de ce fait considérées comme des actes de terrorisme, et Israël se réserve le droit d'y répondre aussi bien dans le cyberespace que par des moyens militaires conventionnels[32].

Mais contre qui cette riposte sera-t-elle concrètement dirigée ? Il n'est effectivement pas toujours facile de savoir si un groupe agit de sa propre initiative ou sous l'impulsion d'un Etat. Surtout que parfois, les hackers entretiennent l'ambiguïté à ce sujet, à l'image de l'Equipe des forces de défense israélienne, qui reprennent la dénomination officielle de l'armée d'Israël, ou du groupe *Ezzedine al-Qassam Cyber Fighters*, qui utilisent le nom de la branche armée du Hamas. Ce lien éventuel est d'autant plus difficile à établir que certains de ces mouvements se font connaître lors d'une seule opération, puis restent discrets ou disparaissent même complètement du paysage cybernétique du Moyen-Orient par la suite. C'est le cas, par exemple, de *Cutting Sword of Justice* qui a revendiqué l'attaque contre la compagnie saoudienne d'hydrocarbure Aramco en août 2012 et de *Parastoo* qui s'est dit être à l'origine du piratage des serveurs de l'Agence internationale pour l'énergie atomique (AIEA) en novembre 2012.

Par contre, il est vrai que le lien entre certains Etats et d'autres groupes sont plus connus, comme entre l'Iran et l'*Iran Cyber Army* (ICA) et entre la Syrie et la *Syrian Electronic Army* (SEA). Les similitudes entre l'ICA et la SEA sont d'ailleurs frappantes aussi bien du point de vue des méthodes utilisées, du soutien étatique non-officiel dont les deux organisations bénéficient que des cibles visées. La *Syrian Electronic Army* a effectivement pour objectif de diffuser la parole officielle du régime syrien et de lutter contre tous les groupes susceptibles de se prononcer ou d'agir contre le pouvoir officiel exactement comme l'*Iran Cyber Army* qui semble cependant plus professionnelle et plus compétente.

La SEA possède un site Internet (IP : 213.178.227.152) enregistré selon Margaret Weiss auprès de la *Syrian Computer Society*, que Bachar al-Assad dirigeait avant qu'il ne devienne président, prouvant par conséquent les liens qui unissent ce groupe de hackers aux dirigeants syriens[33]. Or, une recherche

---

[30] Jack Cloherty, « Virtual Terrorism : Al Qaeda Video calls for Electronic Jihad », ABC News, Mai 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UVLyGxc2YWs

[31] Roi Kais, « Kuwwaiti imam : cyber jihad effective », Ynet, 18 janvier 2012, http://www.ynetnews.com/articles/0,7340,L-4177268,00.html

[32] Ilana Curiel, « Deputy FM threatens forceful response to cyber attacks », Ynet, 7 janvier 2012, http://www.ynetnews.com/articles/0,7340,L-4172329,00.html

[33] Margaret Weiss, « Assad's Secretive Cyber Force », The Washington Institute, Policy Watch 1926, 12 avril 2012 http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFQQFjAA&url=http%3A%2F%2Fwww.

sur les noms de domaine syrian-es.org et syrian-es.com par l'intermédiaire de gandi.net indique que le site de la SEA est enregistré auprès de Network Solutions, une entreprise américaine. Il n'est pas inhabituel de voir des sociétés européennes ou nord-américaines héberger des sites d'organisation comme celle-ci ou même de mouvements considérés comme terroristes. Cela pose la question de l'accessibilité de ces sites ou, plus précisément, de leur hébergement par des compagnies occidentales et, du coup, de leur blocage éventuel par elles, en sachant que les sites ciblés trouvent toujours un moyen pour être à nouveau en ligne.

Mais que son site soit enregistré en Syrie ou ailleurs, la *Syrian Electronic Army* bénéficie en tout cas du soutien tacite de Bachar al-Assad qui a fait explicitement référence à elle dans un discours prononcé en juin 2011. La SEA, par contre, ne cesse de répéter qu'elle est totalement indépendante et qu'elle n'agit pas sur ordre du président syrien. Il est particulièrement compliqué de déterminer avec exactitude la nature des relations qu'entretiennent la SEA et le gouvernement syrien. Nous ne pouvons que constater qu'elle mène toujours des attaques qui vont dans le sens des intérêts du régime.

Les opérations menées par ces différents groupes de hackers s'apparentent à du « vandalisme cybernétique » dans la mesure où il s'agit d'attaques DDoS (déni de service distribué) et de « défacement » qui n'ont que des conséquences bénignes[34]. Elles occasionnent certes un coût et une gêne pour les entreprises et les pays touchés mais elles ne compromettent pas la sécurité des Etats visés. Jusqu'ici, aucun de ces mouvements n'a effectivement réussi à s'infiltrer dans des systèmes d'information sécurisés et sensibles. C'est justement ce qu'Al-Qaïda appelait à faire contre les Etats-Unis dans sa vidéo et qu'il souhaiterait pouvoir faire. C'est également ce que le Mouvement de la résistance islamique palestinien (Hamas) et le Hezbollah libanais aimeraient pouvoir mener comme type d'opération.

2) L'intégration de la dimension cybernétique dans le fonctionnement du Hamas et du Hezbollah

Le Hezbollah s'intéresse au cyber depuis plusieurs années. En 2002, déjà, la CIA publiait un rapport précisant que le mouvement libanais préparait des attaques contre les systèmes d'information de pays occidentaux. Le secrétaire général du Parti de Dieu, Hassan Nasrallah, a effectivement très tôt compris l'intérêt de ce domaine qu'il a complètement intégré à sa stratégie en dotant d'ailleurs le Hezbollah d'une unité cybernétique dès les premières années du XXI^{e} siècle. Il est difficile de dater avec précision à quand remonte la création de cette structure mais elle s'est illustrée pour la première fois en novembre 2004 lors du survol du territoire israélien par un drone du Hezbollah. Ce type

---

washingtoninstitute.org%2Fpolicy-analysis%2Fpdf%2Fassads-secretive-cyber-force&ei=fk4iUMbsKsWt0QWy6IHYDA&usg=AFQjCNG2wOCnxPUBATRyapuRGHYExcwhJQ&sig2=5_yVsg9B0lDHRqJ5sH9qvQ

[34] Une attaque par déni de service distribué consiste en la prise de contrôle de plusieurs ordinateurs, appelés zombies, avec lesquels un opérateur formule des requêtes sur un serveur particulier provoquant ainsi sa saturation et son blocage. Le « défacement » est un anglicisme qui désigne une technique qui vise à défigurer un site web en modifiant par exemple sa page d'accueil pour y introduire un message politique ou une menace. C'est une forme de détournement du site à des fins politiques ou autres.

d'initiative s'est par la suite répété plusieurs fois. Ainsi, le 14 octobre 2012, l'aviation israélienne bombardait au-dessus du Negev un drone qui avait décollé du Liban 3 heures plus tôt et qui semblait effectuer une mission de renseignement. Lors d'un discours prononcé à la télévision, Hassan Nasrallah a confirmé les accusations israéliennes contre l'Iran en affirmant que l'appareil était de fabrication iranienne.

L'implication de Téhéran n'est pas surprenante au regard des relations qu'entretiennent le Hezbollah et l'Iran. Elle est d'ailleurs connue et confirmée depuis la guerre qui a opposé Israël et le mouvement libanais durant l'été 2006[35]. Lors de ce conflit, les militaires israéliens ont été particulièrement surpris par le savoir-faire du Hezbollah en matière cybernétique et par son avance technologique. Depuis cette guerre, le mouvement libanais a profondément amélioré ses compétences, surtout que l'Iran a, de son côté, très rapidement progressé dans le domaine offensif. Le transfert de connaissances entre Téhéran et le Hezbollah reste toutefois difficile à évaluer même si leur collaboration ne fait aucun doute et que le drone lancé par le Hezbollah en octobre 2012 démontre que cette coopération ne s'est effectivement pas arrêtée après la guerre de 2006.

D'ailleurs, elle s'est même étendue au Mouvement de la résistance islamique[36]. Durant l'opération « Pilier de défense » de novembre 2012, l'armée israélienne a bombardé plusieurs usines de drones dans la Bande de Gaza, soulignant ainsi les capacités cybernétiques du Hamas et posant la question de ses relations avec l'Iran, la Syrie et le Hezbollah dans ce domaine. La construction de drones suppose effectivement que le Hamas dispose non seulement de l'infrastructure matérielle nécessaire au fonctionnement de ces appareils, en d'autres termes de stations de contrôle équipées et opérationnelles, mais aussi du personnel qualifié pour le pilotage et pour l'analyse des images transmises aux stations au sol[37].

Ne disposant pas encore de tous ces éléments, le Hamas a donc un effort considérable à faire en termes de formation. Pour le moment, le mouvement dispose d'une unité cybernétique dont les compétences restent encore fragiles. Il ne serait d'ailleurs pas étonnant de voir les dirigeants *hamsaoui*[38] lancer une campagne de recrutement auprès des hackers de la bande côtière pour les intégrer à sa structure et bénéficier ainsi de leur savoir-faire. L'un des groupes les plus actifs dans la Bande de Gaza est le *Gaza Hacker Team,* qui dispose d'un site Internet, d'une page Facebook et qui a revendiqué plus de 1726 attaques depuis janvier 2011, principalement contre Israël, les Etats-Unis et la France[39]. Cependant, les hackers de Gaza n'ont pas les connaissances nécessaires au pilotage de drones et à l'analyse des images. Pour les Israéliens, il ne fait aucun doute que les membres du Hamas seront formés à ces techniques par des spécialistes iraniens à l'image de ce qui a été fait pour le Hezbollah au Liban.

---

[35] Pour plus de détails voir le chapitre 4 de cette étude dans lequel la guerre de 2006 est abordée de manière plus précise.

[36] Pour en savoir plus sur les relations entre le Hezbollah et l'Iran et sur l'unité chargée au sein du parti de Dieu d'apporter un soutien aux mouvements palestiniens, voir l'excellent livre de Matthew Levitt : « Hezbollah : the global footprint of Lebanon's Party of God », George Tow University Press, 368 p.

[37] Il s'agit de la strate sémantique du cyberespace décrite par Jean Loup Samaan, *op. cit.*, p. 830.

[38] Un *hamsaoui* est un membre du Hamas.

[39] Le Gaza Hacker Team a archivé la totalité de ses attaques sur un site Internet : http://www.zone-h.org/archive/notifier=Gaza%20Hacker%20Team

Plusieurs éléments indiquent en tout cas que le mouvement palestinien est dans une phase d'acquisition de ses compétences et qu'il a commencé à intégrer le cyber dans la panoplie de ses outils offensifs. Pour ce qui concerne l'aspect défensif, certaines mesures prises par le Hamas laissent penser que la réflexion n'est pas encore arrivée à maturité mais qu'une prise de conscience est en cours. Le 11 décembre 2012, les autorités de la Bande de Gaza ont ainsi exigé des 10 fournisseurs d'accès à Internet présents sur le territoire côtier d'arrêter de travailler avec des compagnies israéliennes. Evoquant principalement un enjeu économique, lié à la compétition avec Israël, c'est en réalité un souci sécuritaire qui a motivé cette décision. Elle s'inscrit d'ailleurs dans une loi adoptée en septembre 2012, par le gouvernement *hamsaoui*, obligeant les fournisseurs d'accès à Internet à interdire les sites pornographiques sous peine de fermeture. Une loi similaire avait été votée en 2008 mais elle était restée sans effets.

Si le Hamas souhaite exercer un contrôle sur son réseau Internet, celui-ci est également utilisé par le mouvement à des fins de communication. Le Mouvement de la résistance islamique possède effectivement de nombreux sites de nature diverse. Certains sont consacrés à la diffusion de son idéologie et de ses analyses, d'autres sont des sites d'information. Plusieurs sites sont également dédiés à sa branche armée, les Brigades Ezzedine al-Qassam. Le Hezbollah s'inscrit d'ailleurs dans la même stratégie. Outre sa chaîne télévisée, Al-Manar, créée en juillet 1991, sa radio, Al-Nour, lancée en mai 1988, le Parti de Dieu possède plus d'une cinquantaine de sites Internet répartis en différentes catégories : les sites d'information, comme Moqawama, Al-Manar et Al-Intiqad, le quotidien du Hezbollah, les sites locaux, comme Bint-Jbeil, Taybeh, Houla et les sites consacrés aux organisations affiliées au Hezbollah et aux organismes sociaux du mouvement chiite comme Mu'assasat al-shahid[40].

Pour le Parti de Dieu, comme pour le Hamas d'ailleurs, Internet est un outil de communication qui contribue à la « guerre psychologique » contre les ennemis et qui vise à conquérir « les cœurs et les esprits ». Il s'agit pour eux, en d'autres termes, d'un outil de propagande puissant[41]. C'est d'ailleurs pour cette raison que la plupart de ces sites sont accessibles en arabe, en anglais, en espagnol mais aussi en français et en hébreu et qu'ils sont visés régulièrement par des opérations cybernétiques dont le but est de bloquer leur accès aux internautes. Les attaques par déni de service distribué sont fréquents au Moyen-Orient et tous les acteurs de la région, Etats comme groupes non-étatiques, utilisent cette technique. Des groupes qui ne sont pas par nature du Moyen-Orient participent également à cette dynamique. Anonymous est de ce point de vue un exemple parfait. L'originalité toutefois de ce collectif de hackers réside dans le fait que son implication dans la région ne s'arrête pas là.

[40] Pour plus de détails sur ces sites Internet et leurs objectifs, voir l'étude menée par un organisme israélien, le Centre d'Information sur les Renseignements et le Terrorisme, en décembre 2006 :
http://www.terrorism-info.org.il/data/pdf/PDF_18674_3.pdf

[41] La nature des informations et des documents mis en ligne est très variée. Le Hamas par exemple publie de cette manière des manuels destinés à la jeunesse comme Al-Fateh. Voir le rapport réalisé à ce sujet par IMPACT-SE et disponible en ligne sur http://www.impact-se.org/docs/reports/Hamas/Al-Fateh_Francais.pdf

3) Les Anonymous, acteur mineur mais particulièrement actif au Moyen-Orient

Anonymous est un collectif de hackers qui regroupe aussi bien des pirates informatiques du Moyen-Orient que de l'extérieur de cette région. La plupart du temps, ses interventions se limitent à des attaques par déni de service distribué ou à des « défacements » mais depuis son implication dans le soulèvement populaire de Tunisie, fin 2010 - début 2011, Anonymous a diversifié ses formes d'engagement en apportant également un soutien logistique aux populations qu'il souhaite aider. En Tunisie, le mouvement ne s'est effectivement pas contenté de participer à des opérations de piratage, il a aussi appris aux opposants au régime de Ben Ali à partager des vidéos en ligne et à cacher leur identité sur Internet afin de ne pas se faire repérer par les autorités. Il a distribué des manuels en arabe mais aussi en français pour que tous les Tunisiens puissent avoir accès à ces informations. Anonymous a également développé un script Greasemonkey[42] afin que les opposants ne se laissent pas prendre par la campagne de *fishing*[43] organisée par le gouvernement tunisien.

Le groupe s'est donc véritablement investi prenant progressivement dans ses vidéos un ton plus engagé politiquement. En Egypte, Anonymous a travaillé avec Telecomix, un autre collectif de hackers, pour aider les opposants à restaurer les proxys et les sites bloqués par le pouvoir. Ils ont également été particulièrement actifs au moment des coupures de réseaux décidées par le président Moubarak, allant même jusqu'à utiliser les fax pour communiquer avec les Egyptiens sur le terrain. L'action des Anonymous en Egypte ne s'est pas arrêtée après la chute de Moubarak comme l'illustrent les nombreuses menaces lancées à l'encontre des Frères musulmans et du président Morsi.

Lorsque cette vague de contestation populaire a touché la Syrie, en mars 2011, Anonymous a lancé très rapidement une vaste opération de soutien aux opposants à Bachar al-Assad. Particulièrement efficace en raison de l'expérience acquise en Tunisie et en Egypte mais aussi en Iran en 2009, Anonymous, avec l'aide d'autres groupes de hackers, s'en est pris régulièrement aux intérêts du gouvernement syrien. Mais contrairement à l'Egypte ou à la Tunisie, en Syrie la *Syrian Electronic Army* a répliqué contre Anonymous. La SEA s'est ainsi introduite en juillet 2012 dans deux sites liés au mouvement et y a piraté plus de 700 comptes appartenant à ses membres. En Syrie, comme auparavant en Tunisie ou en Egypte, Anonymous a apporté aux opposants une véritable assistance technique et un soutien logistique régulier.

Anonymous a également revendiqué le piratage qui a permis à Wikileaks de publier en juillet 2012 les *Syrian files*. Composés de millions de mails (2 484 899 exactement), écrits entre août 2006 et mars 2012, ces documents montrent selon Anonymous et Wikileaks le double jeu des entreprises occidentales qui ont continué à fournir au pouvoir syrien du matériel de communication et de cyber sécurité malgré le début des affrontements. Anonymous a aussi visé les dirigeants syriens en publiant sur Internet les adresses mails et les mots de passe de presque 80 d'entre eux. Quelques jours plus tard, c'était au tour du président al-Assad lui-même d'être visé par le collectif de hackers qui a piraté

[42] Un Greasemonkey est une extension, pour le navigateur Firefox, qui permet de modifier une page Internet pour changer son apparence, ajouter ou enlever des fonctionnalités.

[43] Le fishing ou hameçonnage est une technique visant à voler l'identité d'une cible ou à obtenir des informations confidentielles de celle-ci à partir d'un subterfuge (courriels corrompus, page Internet falsifiée par exemple).

ses mails et les a transmis aux opposants syriens qui les ont d'ailleurs rendus publics assez rapidement.

Anonymous est intervenu en Tunisie, en Egypte, en Syrie mais aussi au Bahreïn et au Yémen. Tous ces exemples montrent comment un mouvement de hackers, pourtant extérieur à la région, tente d'influencer les affaires internes d'un pays en utilisant ses connaissances et ses compétences cybernétiques. Anonymous attaque effectivement tous les pays du Moyen-Orient et intervient dès qu'il le juge nécessaire en expliquant qu'il lutte contre des gouvernements opaques accusés d'agir dans leur propre intérêt plutôt que dans celui de leur population. C'est d'ailleurs pour cette raison qu'en novembre 2012, quand le gouvernement israélien lance l'opération « Pilier de défense », Anonymous réagit tout de suite en lançant un ultimatum à Israël accusé de mener une agression contre le peuple palestinien. C'est aussi pour cette raison qu'Anonymous attaque en juillet 2012 Dahabshiil, une compagnie internationale de transfert de fonds basée aux Emirats arabes unis, à qui le mouvement reproche de financer le terrorisme.

Il faut toutefois relativiser l'impact des opérations menées par les hackers d'Anonymous. Si leur formation et leur aide technique aux populations sur le terrain a effectivement des conséquences, si leurs piratages mettent parfois mal à l'aise les gouvernements concernés, leurs attaques restent de bas niveau et ne remettent pas en cause la sécurité des Etats qui sont de ce point de vue les seuls acteurs capables de mener des opérations véritablement dangereuses.

Partie 2 : Les tensions du Moyen-Orient sous l'angle du cyber

Chapitre 3 : L'intérêt stratégique de l'outil cybernétique

Les mouvements islamistes du Moyen-Orient trouvent un intérêt à l'outil cybernétique dans 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. Qu'il s'agisse d'Al-Qaïda, du Hezbollah, du Hamas et des autres groupes de la région, ces cinq champs d'action constituent effectivement la base de leur activité cybernétique et vient en complément d'outils dont ils disposaient déjà auparavant[44]. Les Etats aussi n'ont pas attendu de disposer de tels moyens pour mener des opérations de renseignement et de sabotage. En fait, le cyber se greffe à d'anciennes pratiques en permettant toutefois de rendre celles-ci plus performantes. Les modalités d'actions des Etats et des groupes non-étatiques en sont ainsi affectées tout comme la conduite des opérations militaires par les armées.

1) Le cyber, une arme stratégique de communication

Comme nous l'avons vu pour le Hezbollah ou le Hamas, la maîtrise de la dimension « communication » du cyber est, pour certains mouvements, aussi importante que de disposer de moyens militaires efficients étant donné qu'elle s'intègre dans une guerre psychologique qui vise non seulement à endommager le moral de l'adversaire mais aussi à conquérir les cœurs et les esprits. De ce point de vue, les groupes non-étatiques ne sont pas les seuls concernés, les Etats aussi voient leur intérêt dans l'utilisation de telles méthodes. Ce n'est bien entendu pas une nouveauté due à l'émergence des nouvelles technologies - de tout temps la notion de propagande et de contre-propagande a fait partie des relations internationales - mais l'essor de ces moyens techniques permet une diffusion plus étendue et une exposition plus large des discours officiels de chacun de ces acteurs.

Al-Qaïda dans la péninsule arabique (AQPA) a par exemple réalisé « plusieurs films dans lesquels il présentait plusieurs portraits et entrevues de militants, notamment Wabsaya al-Abtal (Testaments des héros) et Shuhada al-Muwajahat (Martyrs des affrontements) ». Les groupes affiliés à Al-Qaïda ont effectivement « leurs propres sites Web et leurs propres centres de production vidéo »[45]. Ces vidéos sont ensuite mises sur Internet, via des plates-formes comme YouTube et Dailymotion et via des forums jihadistes. Al-Qaïda possède effectivement ses propres sites Internet sur lesquels les contenus ne se limitent d'ailleurs pas qu'à la vidéo. Le mouvement y publie des textes détaillant son idéologie, ses revendications et ses moyens d'action. Le public visé est large. Il concerne aussi bien les groupes qui souhaiteraient rejoindre le mouvement que l'individu qui aimerait agir pour celui-ci. Sa revue en

[44] Voir sur ce sujet le rapport de l'Institute for Security Technology Studies (ISTS), « Examining the Cyber Capabilities of Islamic Terrorist Groups », Darthmouth College, 2003, http://www.ists.dartmouth.edu/docs/ITB_032004.pdf

[45] Canadian Center for Intelligence and Security Studies, « La stratégie médiatique et de propagande d'Al-Qaïda », volume 2007-2, p.16. Disponible en ligne : http://itac.gc.ca/pblctns/tc_prsnts/2007-2-fra.pdf

ligne, *Inspire*, propose d'ailleurs des instructions pour apprendre à monter son propre engin explosif[46].

Jusqu'aux attentats du 11 septembre 2001, Al-Qaïda utilisait principalement les médias arabes, et notamment la chaîne d'information qatarie Al Jazeera, comme support de communication. Ce n'est véritablement qu'après 2001, pour rentabiliser l'impact des attentats de New York, qu'Al-Qaïda a décidé d'utiliser massivement Internet. La vidéo, les textes, les forums sont donc devenus des vecteurs très forts de propagande servant aussi bien à créer de l'émulation dans ses rangs qu'à convaincre les autres mouvements jihadistes de la force de ses actions et de la légitimité de celles-ci. Il suffit de lire le 2e numéro d'*Inspire*, mis en ligne le 21 mars 2011 par la branche communication d'AQPA, Al-Malahem Media, pour s'en rendre compte. L'impact réel de ces méthodes est difficile à évaluer mais elles ont en tout cas conduit les Américains à mener une opération cybernétique d'ampleur contre les sites Internet d'Al-Qaïda au Yémen.

Elles ont également poussé les Israéliens à bombarder le bâtiment d'Al-Manar au Liban durant la guerre de 2006 et d'Al-Aqsa TV, la chaîne du Hamas dans la Bande de Gaza, durant l'opération « Plomb Durci » en 2008-2009 mais sans pour autant interrompre durablement le flux d'informations émis par ces structures. Durant la guerre de novembre 2012, les Israéliens ont piraté les programmes d'Al-Aqsa TV, en brouillant les images et en interrompant les programmes, avant de se décider finalement à bombarder à nouveau le siège de la chaîne *hamsaoui*. Ceci dit, entre les conflits de 2006 et celui de 2008-2009, Israël a opéré un virage stratégique notable et durable. En effet, en 2006, le Hamas et le Hezbollah avaient largement gagné la guerre de la communication en utilisant parfaitement leur arsenal cybernétique, alors qu'Israël avait fait l'erreur de peu communiquer et de peu utiliser Internet[47].

C'est pourquoi, lors du conflit de 2009, Israël s'est complètement emparé des réseaux. L'armée israélienne a ainsi créé une chaîne, sur YouTube, diffusant de nombreuses vidéos des opérations menées dans la Bande de Gaza. La mise en ligne de ces programmes en hébreu, en anglais et même en arabe, était combinée à des piratages de sites Internet appartenant au Hamas. En raison de la violence de l'offensive militaire et du nombre de morts côté palestinien, Israël n'avait néanmoins pas réussi à mobiliser les opinions en sa faveur. Par contre, cette stratégie a été plus efficace lors de l'opération « Pilier de défense », en novembre 2012. Israël avait effectivement non seulement pris soin de faire le moins de morts civils possible mais il avait aussi largement amélioré sa communication sur les réseaux sociaux et sur Internet.

« Pilier de défense » est de surcroît la première guerre lancée par Twitter. Après avoir tué le chef des Brigades Ezzedines Al-Qassam, Ahmed al-Jaabari, Tsahal a effectivement envoyé deux twitts : « *the IDF has begun a widespread campaign on terror sites & operatives in the #Gaza Strip, chief among them #Hamas & Islamic Jihad targets* » puis « *the first target, hit minutes ago, was Ahmed Al-Jabari, head of the #Hamas military wing* ». Ce que le Hamas a confirmé immédiatement sur le compte Twitter de sa banche armée avant d'envoyer à son tour : « *Occupation opened hell gates on*

[46] Brian Michael Jenkins, « Is Al-Qaeda's Internet Strategy working ? », Rand Corporation, décembre 2011, 7 p. http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT371.pdf

[47] Pour plus de détails voir Thomas Rid et Marc Hecker, « War 2.0 : Irregular Warfare in the Information Age », Praeger Security International, London, 2009, 280 p.

itself ». Quelques minutes après, plusieurs missiles étaient lancés sur une base militaire israélienne de la ville de Beer Sheva. Non seulement ces messages interposés se sont prolongés pendant tout le conflit mais l'armée israélienne a mis en ligne, sur sa chaîne YouTube, la vidéo du bombardement d'Ahmed al-Jaabari. La guerre de novembre 2012 démontre l'importance donnée par les deux camps à la guerre de l'information et à sa dimension psychologique. Cet épisode est effectivement l'exemple par excellence de l'utilisation du cyber dans une stratégie visant à marquer les esprits et à entamer la motivation de l'ennemi.

Le conflit israélo-palestinien donne aussi lieu à des initiatives visant au rapprochement et au dialogue des populations de la région. La conférence internationale pour la paix, organisée en janvier 2012 par l'ancien négociateur israélien Uri Savir, du *Peres Center For Peace*, et par Salah El-Ayan, de Yala Palestine, en est effectivement un bon exemple. Réunissant plus de 50000 membres, ce sommet virtuel rassemblait notamment de jeunes Israéliens, Palestiniens, Irakiens et Saoudiens souhaitant participer à des discussions sur les principaux enjeux du conflit israélo-palestinien, comme la question du futur statut de Jérusalem ou des frontières. L'impact de cette conférence en ligne et de ses possibles retombées en termes de communication étaient tels que le président israélien, Shimon Peres, le président palestinien, Mahmoud Abbas, ou la secrétaire d'Etat des Etats-Unis, Hillary Clinton, pour ne citer qu'eux, ont tous posté des vidéos sur la plate-forme de Facebook qui servait de support à cet évènement.

Cet exemple, un parmi tant d'autres, illustre la place essentielle occupée par les réseaux sociaux et les sites de partage. C'est d'ailleurs pour cette raison que la grande majorité des groupes de hackers, comme les Gaza Hacker Team, des mouvements islamistes, comme le Hezbollah, des armées, comme Tsahal, ont une page Facebook, un compte Twitter et utilisent YouTube pour poster des vidéos. Les réseaux sociaux et les sites de partage sont également devenus une source précieuse de renseignement pour les Etats et les groupes non-étatiques.

2) L'utilisation du cyber à des fins de renseignement

a) Le renseignement en *open-source*

Le renseignement en sources ouvertes (*Open Source Intelligence* ou OSINT) consiste à collecter de l'information non-confidentielle et accessible à tous. Internet n'est pas la seule source possible pour l'OSINT mais c'est tout de même une cible privilégiée au regard de la densité d'information disponible sur le réseau. C'est d'ailleurs pour cette raison que les Etats du Moyen-Orient et les mouvements islamistes de la région l'utilisent pour recueillir du renseignement.

Le Hezbollah a ainsi créé, par exemple, un faux profil sur Facebook pour obtenir des informations sensibles sur Israël[48]. Un opérateur du Parti de Dieu se faisait passer pour une jeune militaire israélienne, Reut Zukerman. Cette belle et séduisante jeune femme invitait des soldats israéliens, dont la plupart occupaient des postes au sein des services de renseignement, à devenir

[48] Von Sarah Stricker, « Online-Spionage: Die schöne Facebook-Freundin der Elitesoldaten », Der Spiegel, Mai 2010, http://www.spiegel.de/politik/ausland/online-spionage-die-schoene-facebook-freundin-der-elitesoldaten-a-694582.html

amis puis discutait avec eux, dans un hébreu parfait, de leur expérience commune au sein de l'armée, des exercices d'entraînement de leur unité et de la base dans laquelle ils étaient. La supercherie a été découverte suite à la suspicion de certains militaires qui ont décidé d'avertir leur hiérarchie. Le faux profil a été fermé très rapidement après.

Ce n'est pas la première fois que des informations sensibles à propos d'Israël circulent sur Facebook. Au début de l'année 2010, un soldat israélien avait été condamné à 10 jours de prison pour avoir posté plusieurs messages, dont certains relatifs au lancement d'une opération confidentielle en Cisjordanie. Pour les armées, comme pour les groupes non-étatiques, les réseaux sociaux constituent un risque qu'ils doivent apprendre à gérer. Mais pas uniquement[49]. Les bénéfices en termes de recueil de l'information sont également notables. L'exemple du faux profil du Hezbollah illustre la manière dont certains services, en discutant très librement avec des membres de Facebook, obtiennent du renseignement et recrutent même parfois des agents.

Les réseaux sociaux sont également un très bon outil pour juguler, et donc surveiller, des populations. Israël a d'ailleurs effectué une veille poussée sur les meneurs des manifestations sociales qui se sont déroulées dans le pays en 2011 et 2012. Les pays arabes font de même avec les leaders de l'opposition et ces méthodes se sont généralisées dans les Etats où la population s'est soulevée contre ses dirigeants comme en Iran, en Syrie, en Egypte ou au Bahreïn. Les opposants à ces régimes ne sont d'ailleurs pas en reste. En Syrie, ils bénéficient de l'aide de groupes de hackers, syriens mais aussi étrangers, qui s'investissent pour leur fournir de la documentation. Par ailleurs, les informations mises en ligne par certaines plates-formes, dont le but est principalement de communiquer sur ce qui se passe sur le terrain, permettent d'appréhender l'évolution de la situation de manière plus entière et moins fragmentée[50]. Ces informations sont utilisées aussi bien par des services de renseignement étrangers que par les hommes qui combattent l'armée régulière syrienne leur permettant ainsi d'avoir une vision globale de l'ensemble des fronts. Elles sont également utilisées par des activistes, là encore pas nécessairement syriens, pour répartir des informations multiples et variées aux membres du Conseil national syrien (CNS), l'autorité politique qui représente une partie de l'opposition à Bachar al-Assad, et aux dirigeants étrangers afin d'essayer de les mobiliser en faveur des opposants[51].

L'outil par excellence de collecte du renseignement par les mouvements non-étatiques, dont les ressources sont par définition limitées, est le service de Google Earth, qui est une véritable banque de données d'images photographiques et satellites. En 2006, l'Armée islamique, un groupe salafiste présent en Irak, postait sur un site jihadiste une vidéo pour expliquer comment il utilisait Google Earth dans le cadre de ses attaques de roquettes contre les militaires américains. Selon la *Fondation*

[49] Sur la question des risques et des bénéfices des réseaux sociaux pour l'armée voir Marc Hecker et Thomas Rid, « les armées doivent-elles craindre les réseaux sociaux », dans Politique étrangère, « l'Internet outil de puissance », IFRI, n°2, 2012, pp. 317 à 328.

[50] Bambuser est très actif sur la guerre civile syrienne. Des vidéos sont mises en ligne à intervalle très court entre-elles sur l'adresse http://bambuser.com/broadcasts?broadcasts-tabs=middle-east. Lara Setrakian a pour sa part lancé un projet visant à mieux comprendre les évènements syriens sur l'adresse http://beta.syriadeeply.org. Les informations y sont régulièrement mises à jour.

[51] Pour le cas libyen, qui garde toutefois toute son originalité par rapport à la Syrie, voir l'interview par David Millian de Stéphanie Lamy : « Médias sociaux et printemps arabes : plongée dans le 2.0 au cœur de la révolution lybienne », http://comfluences.net/2012/05/31/medias-sociaux-et-printemps-arabe-plongee-au/

of American Scientists, le logiciel de Google n'avait été jusque-là évoqué que sur les forums jihadistes[52]. C'était donc la première fois qu'un mouvement se filmait en utilisant Google Earth et diffusait un vrai tutorial sur la manière de procéder. Néanmoins, cette façon de faire était déjà utilisée par d'autres groupes. Ainsi, durant la guerre de 2006 entre Israël et le Hezbollah, le mouvement chiite s'est servi de Google Earth pour repérer l'emplacement de certaines bases militaires israéliennes. Les groupes jihadistes en Syrie, et notamment le principal et le plus important d'entre eux, Jahbat al-Nosra, opère aussi de cette manière pour identifier ses cibles et organiser ses attentats[53].

b) Le renseignement par virus informatiques

L'ensemble de ces différentes techniques concerne le renseignement en sources ouvertes qui est, par définition, public et disponible à tous. Par contre, la création et la diffusion de virus informatiques est un moyen plus technique de collecte de l'information. Les exemples d'utilisation de ce type de malwares par les autorités des pays de la région sont nombreux. Aux Emirats arabes unis, par exemple, un virus informatique, envoyé par l'intermédiaire d'un mail qui contenait un lien corrompu vers une vidéo, a touché un membre de l'opposition en janvier 2013. Il permettait notamment à ses concepteurs d'avoir accès aux mots de passe et à tout ce qui s'affichait sur l'écran de la victime. En Syrie, cette technique est couramment pratiquée par le gouvernement de Bachar Al-Assad qui développe et diffuse de nombreux virus. L'un d'entre eux, un cheval de Troie[54] appelé *BlackShades*, a été signalé le 20 juin 2012 par l'*Electronic Frontier Foundation* (EFF), une entreprise californienne, et le *Citizen Lab* de Toronto[55]. Il circulait sous l'apparence d'un fichier vidéo dont l'ouverture provoquait l'installation d'un programme permettant ainsi l'accès aux données de la personne visée[56].

Il existe toutefois des virus informatiques plus sophistiqués et plus puissants que ceux utilisés aux Emirats arabes unis ou en Syrie[57]. *Flame* est l'exemple par excellence de ce type d'outils cybernétiques. Découvert par hasard en mai 2012 par la société Kaspersky, *Flame* est le logiciel

---

[52] Fondation of American Scientists, Iraqi Insurgency Group utilizes Google Earth for attack planning », juillet 2006, http://www.fas.org/irp/dni/osc/osc071906.pdf

[53] A propos des mouvements salafistes en Syrie, voir l'excellent rapport de l'*International Crisis Group*, « Tentative Jihad : Syria's fundamentalist opposition », Middle East Report n° 131, 12 octobre 2012, http://www.crisisgroup.org/~/media/Files/Middle%20East%20North%20Africa/Iraq%20Syria%20Lebanon/Syria/131-tentative-jihad-syrias-fundamentalist-opposition.pdf

[54] Un cheval de Troie est un logiciel qui se présente sous une forme honnête, utile ou agréable, et qui une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses. Cette définition est issue du livre de Laurent Bloch et Christophe Wolfhugel, « Sécurité informatique, principes et méthodes à l'usage des DSI, RSSI et administreurs », Eyrolles, 2009, p. 60.

[55] Morgan Marquis-Boire et Seth Hardy, « Syrian Activists Targeted with BlackShades Spy Software », juin 2012, https://citizenlab.org/wp-content/uploads/2012/08/06-2012-syrianactiviststargeted.pdf

[56] Pour une analyse détaillée de ce malware voir l'article écrit pour l'*Electronic Frontier Foundation* par Eva Galperin et Morgan Marquis-Boire, « New malware targeting Syrian Activists uses BlackShades commercial trojan », EFF, 12 juillet 2012, https://www.eff.org/deeplinks/2012/07/new-blackshades-malware

[57] Nous nous bornerons dans ce chapitre aux caractéristiques techniques et surtout aux effets de ces virus afin d'en souligner leur intérêt stratégique. La réflexion sur leur rôle dans les conflits du Moyen-Orient sera abordée dans le chapitre suivant.

malveillant le plus sophistiqué connu à ce jour. D'une taille de 20 Mb, alors que *Stuxnet* ne fait que 500 Ko, il est composé d'au moins 20 modules dont chacun a un rôle bien précis. *Microbe*, par exemple, permet les enregistrements audio alors que *Security* détecte les programmes dangereux pouvant éventuellement conduire à une détection de *Flame* dans le système corrompu. Le module le plus surprenant est nommé *Beetlejuice.* Il est capable de repérer les appareils connectés en Bluetooth à la machine infectée et d'en exfiltrer les données. Ce malware est de loin l'outil d'espionnage le plus performant connu actuellement.

Flame est à l'origine de la découverte de deux autres virus tout aussi efficaces. En effet, en travaillant sur *Flame* les équipes de Kaspersky découvrent un élément qu'ils considèrent au départ comme un simple module supplémentaire avant de se rendre compte, vers juin/juillet 2012, qu'il s'agit d'une structure plus particulière, composée elle-même de plusieurs modules. Ils lui donnent le nom de *Gauss.* Il s'agit en fait d'un cheval de Troie, probablement créé au milieu de l'année 2011 et déployé à partir d'août-septembre de la même année contre des systèmes bancaires, des réseaux sociaux et des comptes e-mail au Liban, en Israël et dans les Territoires palestiniens. Le nombre limité de banques libanaises touchées par *Gauss* permet toutefois de supposer qu'il ne s'agissait pas d'un espionnage à caractère criminel mais bien d'une opération de renseignement ciblée dont le but était certainement de mieux comprendre les activités financières du Hezbollah et de son allié iranien.

Le deuxième virus découvert grâce à *Flame* semble aussi correspondre au profil d'un malware utilisé dans le cadre d'une opération de renseignement ciblée. Connu sous le nom de *MiniFlame*, en raison de sa taille réduite et de ses fonctionnalités, ce virus semble effectivement avoir été conçu pour recueillir des renseignements précis alors que *Flame*, lui, récupérait de l'information en masse. Il n'est donc pas surprenant que 5000 machines aient été infectées par *Flame* alors que seulement une cinquantaine l'ont été par *MiniFlame*. Ces trois virus, *Flame, MiniFlame* et *Gauss*, partagent des similitudes dans leur conception technique. Selon les équipes de Kaspersky, ils sont d'ailleurs basés sur le même type de programmation. La plateforme de *Duqu* par contre correspond à celle de *Stuxnet*. *Duqu* a été détecté en septembre 2011. Il a surtout touché l'Iran où il a volé de nombreuses données sur les systèmes de contrôle industriel du pays et sur les relations commerciales de plusieurs organisations iraniennes. Pour certains experts, *Duqu* a été élaboré en vue de la préparation d'une attaque cybernétique massive sur l'Iran.

Le régime de Téhéran est en tout cas clairement ciblé par *Duqu*, *Flame*, *MiniFlame* et *Gauss* qui ont tous cherché à leur manière à obtenir des informations sur les activités iraniennes et sur les infrastructures critiques de ce pays. Le seul virus utilisé à des fins de renseignement, soupçonné de fabrication perse, *Mahdi*, n'échappe pas pour autant à cette règle. Découvert par l'entreprise de sécurité informatique israélienne Seculert en février 2012, *Mahdi* collectait effectivement différents types d'information sur des structures et des personnes en Iran ayant des liens avec les Etats-Unis, en ciblant tout particulièrement des étudiants, des ambassades et des structures financières. Outre l'Iran, *Mahdi* a principalement touché l'Afghanistan et Israël. Il s'est répandu dans ces trois pays de manière moins élaborée que *Duqu*, *Flame*, *MiniFlame* ou *Gauss*. D'un point de vue technique, *Mahdi* est en effet clairement moins sophistiqué que ces quatre virus. Il s'est propagé à partie d'e-mails malicieux, qui comprenaient des fichiers PDF, JPEG et Power Point corrompus.

L'ensemble de ces virus informatiques démontrent que le renseignement par des moyens cybernétiques est une réalité au Moyen-Orient depuis plusieurs années, d'autant plus que si la découverte de ces malwares est récente, la date de leur création et le temps durant lequel ils ont été actifs sont eux bien plus long. Ce qui veut dire que les pays à l'origine de ces virus disposent d'équipes en permanence actives pour effectuer des mises à jour et traiter les données récoltées. L'utilisation de tels moyens ne se limite toutefois pas à la seule dimension du renseignement.

3) Le cyber comme outil de sabotage

Gauss entre également dans cette catégorie étant donné qu'il dispose d'un module, appelé Godel, qui peut attaquer des systèmes SCADA (*Supervisory Control and Data Acquisition*) qui sont des systèmes automatiques organisant certaines infrastructures, notamment dans les secteurs de l'eau, des transports et des finances. En d'autres termes, *Gauss* n'est pas qu'un logiciel espion, il peut aussi infliger des dommages physiques.

Cette double compétence, espionnage et sabotage, n'est toutefois pas particulière à *Gauss*. Le malware qui s'est attaqué en août 2012 à la compagnie saoudienne d'hydrocarbure Aramco dispose aussi de ces mêmes caractéristiques. Selon la compagnie israélienne Seculert, ce virus informatique, appelé *Shamoon*, opère en deux phases distinctes[58]. Dans un premier temps, il prend le contrôle d'une machine directement connectée à Internet et à partir de cet appareil il contamine les autres ordinateurs qui, eux, ne sont pas obligatoirement reliés à l'extérieur. Puis, dans un second temps, une fois que *Shamoon* s'est répandu dans tout le système, il est activé par son opérateur. A partir de là, il récupère les données qui l'intéressent et les supprime ensuite des disques durs des ordinateurs qu'il a infectés. C'est de cette manière que *Shamoon* a endommagé près de 30 000 stations de travail, soit 75% des ordinateurs d'Aramco qui a mis plus de deux semaines avant de pouvoir restaurer la totalité de son système.

A l'instar de *Mahdi*, *Shamoon* a été inoculé par *fishing* ce qui est assez surprenant car son efficacité aurait été accrue par un moyen plus discret, tel que l'exploitation d'une vulnérabilité des systèmes d'Aramco. Cet élément permet de supposer que l'équipe à l'origine de ce virus informatique ne disposait pas de toutes les qualifications nécessaires même si ces concepteurs ne sont pas pour autant des amateurs. En effet, si l'analyse technique de *Shamoon* n'a pas clairement établi la responsabilité d'un Etat, il est peu probable selon les spécialistes qu'un simple groupe de hackers puisse en avoir assuré l'élaboration pour autant. Par contre, tout semble indiquer que *Shamoon* a été conçu en s'inspirant d'un autre virus, appelé *Wiper*, qui s'est attaqué en avril 2012 aux installations pétrolières iraniennes. Or, les créateurs de *Wiper* ont pris soin de le doter d'un système de sécurité effaçant les traces de son passage. Du coup, les informations disponibles sur lui sont rares étant donné que les sociétés de sécurité informatique ne disposent que de très peu de matériel sur lequel baser leur analyse. Ses caractéristiques techniques et ses capacités de destruction en font toutefois un outil bien plus efficace que *Shamoon* qui reste moins sophistiqué que d'autres virus informatiques ayant touché les pays de la région.

[58] Seculert, « Shamoon, a two-stage targeted attack », 16 août 2012, http://blog.seculert.com/2012/08/shamoon-two-stage-targeted-attack.html

En revanche, *Stuxnet* constitue certainement l'outil cybernétique utilisé à des fins de sabotage le plus complexe connu jusqu'à aujourd'hui. *Stuxnet* est un ver informatique, c'est-à-dire qu'il évolue de manière autonome à travers les réseaux. Il dispose d'une capacité d'auto-exécution qu'il active seulement une fois sa cible atteinte. *Stuxnet* est le premier logiciel malicieux conçu pour un type spécifique et clairement défini de système de contrôle industriel (SCI)[59]. Il attaque et endommage effectivement un modèle particulier de SCI produit par Siemens, en l'occurrence le modèle SIMATIC, en s'en prenant au logiciel informatique Step7 qui permet de l'utiliser. Il profite dans le même temps d'une vulnérabilité de Windows pour se cacher, ce qui lui permet de rester en toute discrétion dans le système corrompu[60]. Ce modèle de SCI est notamment utilisé par Téhéran. L'Iran est d'ailleurs le pays où les traces de *Stuxnet* sont les plus répandues. D'autres pays ont cependant été touchés, comme la France et l'Inde dont un satellite INSAT-4B, contrôlé par un système SCADA reposant sur des SCI produits par Siemens (S7-400 et SIMATIC), a été déclaré hors service par les autorités indiennes le 9 juillet 2010 sans que l'on sache exactement si *Stuxnet* en était directement responsable. En Iran, par contre, le ver aurait détruit plus de 1000 centrifugeuses IR-1 de l'usine d'enrichissement d'uranium de Natanz, soit 11% des centrifugeuses utilisées à l'époque sur ce site[61]. Les Iraniens ont indiqué, le 25 septembre 2010, avoir repéré près de 30 000 adresses IP d'ordinateurs utilisés dans leur industrie nucléaire infectés par *Stuxnet*.

Les installations nucléaires du site de Bouchehr auraient également été touchées mais sans que l'on sache exactement dans quelles proportions et avec quelles conséquences. Les analyses techniques ont en tout cas montré que *Stuxnet* était composé de nombreux modules dont le module 315, qui ciblerait spécifiquement les centrifugeuses IR-1, et le module 417 qui lui s'attaquerait en particulier au modèle de turbines à vapeur utilisées dans la centrale de production électrique de Bouchehr. Les auteurs de *Stuxnet* auraient donc utilisé un ver informatique pour deux types différents de SCI. La conception de *Stuxnet* n'est pas une entreprise à la portée de tous. Elle suppose de hautes compétences techniques, des renseignements pointus en amont de la programmation afin de bien connaître les caractéristiques des cibles visées et la possibilité de tester le ver avant de l'inoculer afin de s'assurer de sa fonctionnalité. Tout ceci demande donc un budget conséquent, des équipes importantes et des compétences que seuls peu d'Etats ont. Selon le centre de recherche du Congrès des Etats-Unis, les pays disposant des connaissances et des raisons de mener une telle attaque sont « les Etats-Unis, Israël, le Royaume-Uni, la Russie, la Chine et la France »[62].

Stuxnet n'est pas le premier exemple de l'utilisation de moyens cybernétiques à des fins de sabotage. En effet, en 1982, sur la base d'informations des services de renseignement français, les Etats-Unis ont implanté un cheval de Troie dans un système SCADA acheté par l'URSS aux Canadiens. Ce virus informatique aurait provoqué l'explosion du pipeline transsibérien que les Soviétiques étaient

[59] Les systèmes de contrôle industriel, qui organisent l'automatisation de plusieurs infrastructures critiques, comprennent les systèmes SCADA, les systèmes numériques de contrôle-commande et les automates programmables industriels.

[60] Pour une synthèse sur le fonctionnement de *Stuxnet* voir le très bon rapport fait par Paul Mueller et Babak Yadegari, « The Stuxnet Worm », Département des sciences de l'informatique, Université de l'Arizona, http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

[61] *Ibid*, p. 1

[62] Paul K. Kerr, John Rollins, Catherine A. Theohary, *op. cit.*, p. 2.

en train de construire[63]. Ce malware et *Stuxnet* ont pour point commun d'avoir été conçus dans le cadre d'une opération de sabotage servant d'alternative à un recours à la force armée. Or, l'outil cybernétique est également une composante à part entière de plusieurs opérations militaires qui se sont déroulées au Moyen-Orient. La guerre de 2006 entre le Hezbollah et Israël en est un parfait exemple, tout comme le raid mené par l'aviation israélienne contre un site nucléaire syrien, situé près de la ville de Deir Ez Zor, dans la nuit du 5 au 6 septembre 2007[64].

Lors de cette opération, les Israéliens ont effectivement déployés d'importants moyens cybernétiques : « huit chasseurs bombardiers F-15 et un avion de guerre électronique Gulfstream G-550 Nachson […]. Le Gulfstream Nachson est équipé pour assurer la protection électromagnétique des bombardiers et brouiller les systèmes de détection et de communications adverses »[65]. Des chasseurs F-16 intègrent ce dispositif « pour accroître le potentiel de guerre électronique et de lutte anti-radar »[66]. Après avoir décollé d'Israël, cette flotte pénètre en Syrie par la Turquie et aveugle alors la défense anti-aérienne syrienne. Selon Pierre Razoux, la formation se divise à ce moment-là en deux groupes : le premier bombarde la station radar située au sommet du Tel el-Abouad puis fait demi-tour, alors que le deuxième se dirige vers le site nucléaire et le détruit. Richard Clarke et Robert Knake, ne font pas mention du bombardement sur la station radar syrienne. Pour eux, l'aviation israélienne avait le contrôle des écrans radars syriens assurant de cette manière la furtivité de leurs appareils. Ainsi, si la défense anti-aérienne syrienne n'a rien vu c'est parce qu'elle ne pouvait tout simplement rien voir étant donné que rien ne s'affichait sur ses écrans de surveillance :

> « *When the Israelis attacked Syria, they used light and electric pulses, not to cut like a laser or stun like a taser, but to transmit 1's and 0's to control what the Syrian air defense radars saw. Instead of blowing up air defense radars and giving up the element of surprise before hitting the main targets, in the age of cyber war, the Israelis ensured that the enemy could not even raise its defenses* »[67].

Il est difficile de savoir comment les Israéliens ont pris exactement contrôle des systèmes de défense anti-aériens syriens. Richard Clark émet trois hypothèses dont celle de la contamination du réseau par un cheval de Troie activé durant le raid par l'aviation israélienne. Quelle que soit la méthode suivie, les Israéliens ont en tout cas réussi, grâce à leurs compétences cybernétiques, à garder pour eux l'effet de surprise faisant de ce raid un véritable cas d'école. Si Israël devait attaquer les installations nucléaires iraniennes, il est fort probable que les autorités militaires procèderont plus ou moins de la même manière pour aveugler la défense anti-aérienne de la République islamique. D'où le silence israélien sur le déroulement du raid contre la Syrie et en particulier sur la phase de contrôle du ciel syrien.

---

[63] William Saffire, « The Farewell Dossier », The New York Times, 2 février 2004, http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html

[64] Nous reviendrons en détails sur la guerre entre Israël et le Hezbollah dans le chapitre 4.

[65] Pierre Razoux, « Israël frappe la Syrie : un raid mystérieux », *Politique étrangère*, n°1, 2008, IFRI, Armand Colin, Paris, p.11.

[66] *Ibid*, p. 12.

[67] Richard A. Clarke et Robert K. Knake, « Cyber War, the next Threat to National Security and what to do about it », Harper Collins, New York, 2010, pp. 9-10.

Chapitre 4 : Des exemples de conflictualité cybernétique au Moyen-Orient

Le Moyen-Orient est une région conflictuelle au sein de laquelle tous les moyens sont mobilisés par les acteurs de la région pour arriver à leurs fins. Nous retiendrons dans ce chapitre trois exemples de cet état de fait. Le premier concerne la guerre qui a opposé Israël et le Hezbollah en 2006. Elle illustre effectivement la manière dont un mouvement islamiste, grâce à sa collaboration avec un Etat, a su développer ses capacités cybernétiques et les utiliser dans le cadre d'un conflit armé. La guerre civile syrienne est également un théâtre d'affrontement où les forces en présence cherchent à tirer avantage de leurs compétences cybernétiques. Le pouvoir iranien est impliqué aussi bien dans la guerre de 2006 que dans celle en Syrie où il fait profiter ses alliés de ses connaissances. Le dernier exemple est d'ailleurs consacré à l'Iran et à la place particulière qu'il occupe dans les affrontements cybernétiques au Moyen-Orient.

1) Le conflit de l'été 2006 entre Israël et le Hezbollah

L'université Saint-Joseph de Beyrouth a réalisé une étude détaillée et précise sur la dimension cybernétique de ce conflit[68]. Comme beaucoup d'études sur la guerre de 2006, les auteurs de ce rapport abordent en détail l'utilisation d'Internet par les deux camps. Ils soulignent également l'importance donnée à la communication par les belligérants. Comme nous l'avons vu, le Hezbollah a fait de cette question une priorité stratégique dès ses premières années d'existence[69].

Pour Hassan Nasrallah, la dimension communication était aussi importante stratégiquement que d'envoyer massivement des roquettes sur le territoire israélien, surtout que la première phase de l'opération lancée par Israël consistait en un bombardement massif des positions du Hezbollah au Sud-Liban donnant l'impression que le mouvement se trouvait dans une situation critique. Cette guerre de l'information s'inscrit donc complètement dans la guerre psychologique que se sont livrés les deux camps durant toute la durée des combats. Les sites Internet rattachés au Hezbollah ont d'ailleurs multiplié les reportages visant à démontrer que les opérations israéliennes n'avaient pas d'effets sur le mouvement chiite. Lorsque les affrontements au sol ont commencé, les membres du Hezbollah ont continué à poster en ligne des vidéos et des témoignages dont l'objectif était de souligner leur efficacité face à l'armée réputée la plus forte du Moyen-Orient. Face à cette stratégie, des organisations juives se sont mobilisées dans le monde entier pour contrecarrer la parole du

[68] Sabrine Saad, Stéphane B. Bazan, Christophe Varin, « Asymmetric Cyber-warfare between Israel and Hezbollah : the Web as a new strategic battlefield », Université Saint-Joseph de Beyrouth, http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf

[69] Voir la thèse soutenue en mars 2009 par Jacqueline S. Kiel, « Hizbullah's Culture Wars, understanding Hizbullah through social movement theory and its media usage », Naval Postgraduate School, Californie, http://www.dtic.mil/dtic/tr/fulltext/u2/a496945.pdf. Pour comprendre comment cette stratégie a été appliquée lors de la guerre de 2006 voir Marvin Kalb et Carol Saivetz, « The Israeli-Hezbollah war of 2006 : The Media as a weapon in Asymmetrical Conflict », Harvard's Kennedy School of Government, 2007, http://www.brookings.edu/~/media/events/2007/2/17islamic%20world/2007islamforuleur effm_israel%20hezb%20war

Hezbollah et soutenir Israël. Elles ont ainsi appuyé l'Union mondiale des étudiants juifs, dont le siège est à Tel-Aviv, pour l'aider à mettre en place un logiciel, appelé *mégaphone*, visant à centraliser toutes les informations sur les opérations israéliennes et tous les communiqués officiels d'Israël. Ce projet s'est fait en accord avec le Ministère des Affaires étrangères à Jérusalem dont ils avaient obtenu le soutien au préalable.

Le cyberespace n'a pas été qu'un espace de communication dans lequel les deux camps cherchaient à légitimer leurs actions. Il a également été un espace d'affrontement cybernétique plus violent. L'étude de l'université de Saint-Joseph de Beyrouth a effectivement montré que les attaques par déni de service distribué (DDoS) ont été monnaie courante. La majorité des sites ciblés par Israël et le Parti de Dieu l'ont été en raison de leur place dans la stratégie de communication des deux camps. Les hackers du Hezbollah s'en sont ainsi pris à plusieurs sites gouvernementaux et militaires israéliens alors qu'Israël, de son côté, a attaqué durement le site de la chaîne d'information Al-Manar, l'obligeant d'ailleurs à changer d'hébergeur. En toile de fond de cet affrontement cybernétique s'est déroulée une autre bataille entre hackers arabes et israéliens. L'ingérence de groupes de hackers divers et variés dans les conflits du Moyen-Orient est devenue systématique. Ce fut le cas lors du raid mené par l'armée israélienne contre la flottille qui voulait rompre le blocus de Gaza en mai 2010 et lors de toutes les opérations lancées par Israël contre le Hamas en 2006, en 2008-2009 et en 2012[70]. A chaque fois, des hackers, prenant partie pour tel ou tel camp, ont lancé des offensives cybernétiques contre celui jugé comme l'ennemi.

Les attaques DDoS et les « défacements » ne sont qu'un exemple d'outils mobilisés par Israël et le Hezbollah en 2006. Les deux belligérants ont ainsi créé des logiciels malveillants afin d'infecter les données des systèmes d'information du camp opposé. Le Hezbollah a fait usage à plusieurs reprises de *Google Earth* afin d'obtenir du renseignement sur Israël. Tsahal a de son côté cherché à bloquer le réseau Internet libanais afin de perturber le Hezbollah qui s'en servait pour effectuer des transmissions de données, pour communiquer et pour recueillir donc du renseignement. Pour y parvenir, l'armée israélienne aurait utilisé, selon les auteurs du rapport de l'université de Beyrouth, les capacités cybernétiques des navires de guerre qu'ils avaient déployés le long de la côte libanaise. Non seulement les perturbations n'ont pas été efficaces mais en plus le Hezbollah a tiré un missile de type C-801 (de fabrication chinoise mais surement d'origine iranienne) sur la corvette *Hanit*, de la classe Saar V, tuant quatre marins israéliens et obligeant le navire à rentrer en Israël. Le Hezbollah a fait de cette attaque un évènement exceptionnel grâce aux vidéos postées sur Internet.

Outre les tentatives de neutralisation d'Internet, les Israéliens ont également attaqué l'ensemble des réseaux de communication du Sud-Liban, téléphones fixes et mobiles inclus, pensant ainsi rendre muet le Hezbollah. En fait, il n'en a rien été. Selon David Eshel, le Parti de Dieu a bénéficié de l'aide de l'Iran durant le conflit pour protéger ses réseaux de communication[71]. Les soldats israéliens ont effectivement trouvé à Bint-Jbeil des appareils d'écoute et de surveillance et du matériel de

[70] Concernant la dimension cybernétique de l'opération « Plomb Durci » de 2008-2009, voir Jeffrey Carr, « Inside Cyber Warfare », O'Reilly, 2e édition, décembre 2011, pp. 19 à 28.

[71] David Eshel a créé dans les années 1970 une revue, aujourd'hui disponible en ligne, appelée Defense Update. Colonel de réserve de l'armée israélienne, fondateur et directeur de Defense Update, il est connu pour le sérieux de ses articles. Il a d'ailleurs publié un texte particulièrement intéressant sur la dimension cybernétique de la guerre de 2006 : David Eshel, « Hezbollah intelligence War », accessible sur http://defense-update.com/analysis/lebanon_war_1.htm

communication de fabrication iranienne[72]. Ils ont également découvert les corps de trois officiers du renseignement iranien qui participaient au brouillage des radars et des communications de l'armée israélienne. Selon les experts américains et israéliens qui se sont déplacés sur le terrain, l'Iran s'est servi de cette guerre pour tester ses capacités cybernétiques et pour étudier celles d'Israël.

De nombreux spécialistes ont effectivement vu ce conflit comme un affrontement indirect entre Israël et l'Iran en raison de l'implication des autorités iraniennes dans la formation, l'entraînement et les fournitures d'armes au Parti de Dieu. Les Israéliens ont d'ailleurs été surpris par le matériel dont disposait le Hezbollah et par l'ampleur du partenariat entre l'Iran et le mouvement libanais dans le domaine cybernétique. Le mouvement chiite n'est toutefois pas le seul à profiter du savoir-faire iranien. Le pouvoir syrien aussi profite des compétences de Téhéran pour améliorer ses propres connaissances.

2) La guerre civile syrienne

Depuis mars 2011, le président syrien fait face à un mouvement de contestation qui s'est progressivement transformé en guerre civile. Dans ce contexte, chaque camp tente de diffuser sa version des faits, faisant là aussi de la maîtrise de l'information un enjeu majeur du conflit. Un rapport de l'*International Crisis Group* évoque d'ailleurs plusieurs exemples d'éléments erronés ou confus ou tout simplement manipulés par un des acteurs mêlés au conflit[73]. Ainsi, les 10 et 11 juin 2011, des rumeurs de tirs d'hélicoptère sur une manifestation dans le gouvernorat d'Idlib étaient rapportés par certains médias sans que cela puisse être corroboré sur le terrain[74]. Une page Facebook dédiée à la « révolution syrienne », et largement consultée, était en réalité utilisée par les Frères musulmans pour diffuser leurs idées et leurs analyses de la situation en cours[75].

Internet est un outil de choix en termes d'information et de désinformation. C'est d'ailleurs pour cette raison que le pouvoir syrien n'hésite pas à couper et à ralentir régulièrement le réseau. Au début du conflit, ces mesures visaient aussi à compliquer au maximum l'organisation des manifestations par les contestataires syriens tout en empêchant dans le même temps la transmission d'informations aux médias étrangers, mais lorsque la contestation s'est transformée en conflit armé, le pouvoir syrien a utilisé cette technique à plusieurs reprises pour gêner la communication entre les opposants sur le champ de bataille. Ainsi, les coupures d'Internet ont souvent été accompagnées de perturbations des réseaux GSM pour en décupler les effets. C'est ce qui s'est passé fin février 2012 avant que l'armée régulière de Syrie ne lance l'assaut sur le quartier de Baba Amr (Homs). C'est également la stratégie suivie par le pouvoir syrien au moment où les combats s'intensifiaient à

[72] Yaakov Katz, « Army seals off Hizbullah stronghold of Bont Jbail », The Jerusalem Post, http://www.jpost.com/LandedPages/PrintArticle.aspx?id=29385

[73] Le personnel de l'*International Crisis Group* dispose au Moyen-Orient d'un réseau dense et généralement bien informé.

[74] International Crisis Group, « Popular Protest in North Africa and the Middle East : The Syrian Regime's slow-motion, suicide », Report n° 109, 13 juillet 2011, p. 3.

[75] International Crisis Group, « Popular Protest in North Africa and the Middle East : The Syrian People's slow-motion revolution », Report n° 108, 6 juillet 2011, p. 8.

Damas et dans sa banlieue vers la fin novembre 2012. Internet a ainsi été coupé pendant quasiment trois jours et les téléphones fixes et mobiles ne fonctionnaient plus dans certaines régions comme à Homs ou à Hama.

La perturbation du fonctionnement d'Internet n'est pas difficile à réaliser pour les dirigeants syriens. En effet, la Société syrienne des télécommunications (SST ou STE en anglais) est responsable du marché des télécommunications et de l'offre dans ce secteur. C'est elle qui régule l'attribution des licences et qui applique les décisions prises par le Ministère des communications et des technologies. La SST est également le principal fournisseur d'accès à Internet (FAI) du pays ; elle contrôle plus de 95% du réseau. Les 5% restants sont partagés entre Syriatel, une compagnie privée créée en 2000, aujourd'hui le deuxième acteur majeur des télécommunications en Syrie, et les petits FAI qui dépendent de la SST pour leur activité. De par son statut public, la SST est directement rattachée au pouvoir syrien. Syriatel, de son côté, est dirigée par Rami Makhlouf, un cousin de Bachar al-Assad. Les intérêts des deux principaux FAI syriens rejoignent donc ceux du gouvernement qui n'a donc aucune difficulté à leur faire appliquer ses exigences.

La coupure d'Internet est d'autant plus efficace en Syrie que le réseau n'a qu'une dizaine de points d'interconnexion avec l'extérieur alors qu'en Egypte, par exemple, il en avait plus de 200, en janvier 2011, au moment où le président Moubarak avait décidé de couper Internet[76]. En Egypte, la relation des FAI avec le pouvoir n'était également pas la même que celle entretenue entre les FAI syrien et les dirigeants de Damas. Il faut néanmoins relativiser les effets obtenus par de telles décisions en soulignant qu'en Syrie le taux de pénétration de l'Internet tourne autour de 17% seulement et que tout ne se passe pas sur Facebook ou Twitter. Les Syriens qui combattent l'armée régulière ont effectivement mis en place des comités de coordination sur le terrain, qui sont les véritables organes de coordination du soulèvement syrien, et certains médias étrangers, tout comme certains pays occidentaux, ont transmis aux opposants des technologies leur permettant de contourner ces mesures.

Outre la coupure d'Internet et des réseaux GSM à des moments stratégiques, le régime syrien a aussi créé des programmes informatiques offensifs. Il utilise ainsi une technique connue sous le nom de *man in the middle*, qui consiste à intercepter les communications entre deux postes sans qu'aucun des opérateurs ne s'en rende compte. *Infowar Monitor* a rapporté en mai 2011 que ce type d'attaque avait été utilisé en Syrie sur une version sécurisée de Facebook[77]. L'attaquant pouvait donc accéder aux comptes de la victime et à toutes ses conversations. Une autre technique dont s'est servi le pouvoir syrien consiste à saturer de requêtes ou de messages les réseaux, les sites et les comptes jugés hostiles. Ainsi, au début des événements, les Syriens se servaient du compte Twitter « Syria# » pour transmettre des informations sur les manifestations. Or, très rapidement, ce compte a commencé à recevoir des messages pro-régime, des insultes, des menaces et finalement des spam rendant son fonctionnement plus difficile.

Le gouvernement syrien a également développé et diffusé différentes sortes de malwares, comme BlackShades. Il a aussi utilisé des RAT (*Remote Administration Tool*), c'est-à-dire des programmes

[76] Pierre Alonso, « La Syrie, coupure net », OWNI, 7 juin 2011, http://owni.fr/2011/06/07/la-syrie-coupure-net/

[77] *Infowar Monitor* est un centre de recherche canadien né en 2002 du partenariat entre le Citizen Lab de la *Munk School of Global Affairs* de l'université de Toronto et un think tank nommé The SecDev Group basé à Ottawa.

permettant la prise de contrôle totale d'un ordinateur depuis un autre ordinateur. DarkComet, par exemple, est un RAT de fabrication française qui a été modifié pour espionner l'opposition syrienne. Selon Telecomix, le serveur utilisé par cette nouvelle version de DarkComet se trouvait au sein de la Société syrienne des télécommunications. Le développeur de DarkComet, Jean-Pierre Lesueur, a condamné le détournement de son programme et a décidé de ne plus travailler dessus. Cet exemple illustre la dualité des technologies cybernétiques et pose plus généralement la question de la vente de système de sécurité à des pays qui peuvent potentiellement en faire un usage répressif.

Par ailleurs, les dirigeants syriens mobilisent régulièrement des groupes de hackers, comme la *Syrian Electronic Army*, qui mènent des attaques par déni de service distribué (DDoS) ou par « défacement »[78]. La SEA a d'ailleurs créé une page Facebook à destination de tous ceux qui veulent soutenir le pouvoir syrien où elle explique comment mener ce type d'attaques. Certains médias arabes sont régulièrement pris pour cible par la *Syrian Electronic Army*. Le site Internet de la chaîne qatarie Al-Jazeera a par exemple été piraté par la SEA en avril 2012 en même temps que le compte Twitter d'Al-Arabiya, un journal saoudien, qui envoyaient des faux messages évoquant une explosion dans les installations gazières du Qatar, le remplacement du Premier ministre et du ministre des Affaires étrangères du Qatar ou encore l'arrestation de la fille du Premier ministre du Qatar à Londres. La SEA cherchait très certainement à exacerber les tensions qui existent entre le Qatar et l'Arabie Saoudite afin de troubler leur partenariat sur la question syrienne. En janvier 2013, la *Syrian Electronic Army* a annoncé détenir plusieurs documents détaillant le rôle joué par la Turquie, l'Arabie Saoudite et le Qatar dans le monde arabe depuis près de deux ans. Ces informations ont été par la suite diffusées sur le site d'Al-Akhbar, qui est un journal libanais réputé proche du Hezbollah. Ce type d'initiatives est fréquent et les pays visés sont toujours ceux qui prennent officiellement position contre Bachar al-Assad et qui sont accusés par le pouvoir syrien de soutenir militairement l'opposition.

Les opposants au pouvoir en place peuvent effectivement compter sur l'aide de plusieurs acteurs extérieurs au conflit. Dans le domaine cybernétique, ils bénéficient de l'appui d'Anonymous qui s'est particulièrement engagé en Syrie. Ils bénéficient aussi de l'aide de pays occidentaux qui, s'ils rechignent à leur envoyer des armes en raison de la présence dans leur rang de nombreux groupes jihadistes, n'hésitent pas à leur apporter leur soutien dans le domaine cybernétique. Ainsi, selon le *Time*, l'administration Obama fournit aux opposants à Bachar al-Assad des téléphones satellites, des GPS et des technologies permettant de contourner la censure de l'Internet et de garantir leur anonymat[79]. Selon un rapport du département de recherche du Congrès, l'aide américaine comprend également des moyens non létaux comme « du matériel médical, des lunettes à vison nocturne et des équipements de communication »[80].

---

[78] Un article détaillé d'*Infowar Monitor*, en date du 25 juin 2011, retrace les différentes techniques et cibles du groupe. Il est disponible en ligne sur : http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/

[79] Jay Newton-Small, « Hillary's Little Startup: How the U.S. Is Using Technology to Aid Syria's Rebels », Time World, 13 juin 2012, http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/

[80] Jeremy M. Sharp et Christopher M. Blanchard, « Armed conflict in Syria : US and International response », Congressional Research Service (CRS), 19 juillet 2012, http://www.fas.org/sgp/crs/mideast/RL33487.pdf

Les Etats-Unis dispensent également des formations en informatique afin que les opposants apprennent à envoyer leurs films, leurs photos et plus largement leurs témoignages à l'étranger mais aussi pour qu'ils prennent l'habitude d'avoir une bonne « hygiène informatique » afin d'éviter qu'ils ne se laissent trop facilement prendre au piège par des fichiers corrompus. Les Américains ne sont pas les seuls à soutenir les opposants syriens. D'autres pays, à l'instar de la France, ont effectivement proposé leur aide en fournissant par exemple des systèmes de communication sécurisés. Le pouvoir syrien aussi peut compter sur un appui cybernétique solide venant de l'étranger à travers son partenariat avec l'Iran et, même si aucun indice ne permet de l'affirmer avec certitude, avec la Chine et la Russie. Certes, ces moyens ne constituent pas un élément primordial de l'aide destinée à la Syrie mais il n'en reste pas moins que les différents acteurs étrangers mêlés au conflit ont intégré les outils cybernétiques à la liste des besoins du camp qu'ils soutiennent. En cela, le soulèvement syrien se distingue de ceux intervenus en Tunisie, en Egypte et en Libye.

Au Yémen, le problème se pose différemment. Le soulèvement yéménite inclut en effet un deuxième front qui oppose le pouvoir en place et les membres d'Al-Qaïda dans la péninsule arabique. Le Yémen n'étant pas un Etat particulièrement développé du point de vue du cyber, l'avantage dans ce domaine est donc du côté d'AQPA qui bénéficie d'un meilleur savoir-faire. Or, les opérations menées par Al-Qaïda au Yémen reposent surtout sur la dimension communication du cyber face à laquelle le pouvoir en place est particulièrement dépourvu. C'est pourquoi, les Etats-Unis ont pris le relais en s'attaquant directement aux intérêts d'Al-Qaïda. La secrétaire d'Etat des Etats-Unis, Hillary Clinton, a d'ailleurs reconnu en mai 2012, que le *Center for Strategic Couterterrorism Communication*, rattaché au Département d'Etat, avait attaqué les sites Internet d'AQPA pour stopper le flux d'information que le groupe diffusait en ligne.

Ce qui est intéressant dans la démarche américaine, c'est que les Etats-Unis n'ont pas décidé de bloquer l'accès aux sites par des attaques DDoS ou de gêner leur utilisation par des « défacements » mais ils ont préféré changer leurs contenus brouillant ainsi les messages d'Al-Qaïda. Le mouvement aurait d'ailleurs diffusé un texte pour ses sympathisants en leur demandant de ne pas croire tout ce qu'ils trouvaient sur Internet. Plutôt que de mener une opération de communication, les Etats-Unis ont donc souhaité créer le doute étant donné la difficulté pour un internaute d'évaluer la véracité des informations diffusées.

3) Réflexion autour des virus informatiques du Moyen-Orient

Les pays du Moyen-Orient ont été la cible de plusieurs virus sophistiqués qui ont été principalement utilisés à des fins de renseignement et de sabotage. Les traces détectées de *Stuxnet*, *Flame*, *Gauss* et des autres malwares sont effectivement plus présentes au Moyen-Orient qu'ailleurs sur la planète. Cet élément indique que leur utilisation s'intègre pleinement aux rapports de force qui sont en action dans cette région et que leur compréhension doit être rattachée aux enjeux particuliers de la scène moyen-orientale. Cet aspect de la réflexion se confronte à un problème essentiel qui est l'impossibilité d'attribuer avec une certitude absolue l'origine d'une attaque cybernétique. Cette difficulté n'empêche pas toutefois d'émettre des hypothèses mais pour parvenir à un résultat crédible, l'analyse purement technique des malwares ne suffit pas. Il faut effectivement la combiner

avec deux éléments essentiels : l'opportunité et la volonté de l'Etat soupçonné. L'opportunité concerne ses compétences techniques et ses ressources humaines et financières alors que la volonté, ou sa motivation à agir, doit être évaluée en fonction de critères divers comme la perception de cet Etat d'un danger touchant à sa sécurité ou le contexte géopolitique dans lequel il évolue[81].

A partir de ces éléments, à qui peut-on attribuer les différents virus sophistiqués qui se sont répandus au Moyen-Orient ? Existe-t-il d'abord un lien entre eux ou sont-ils complètement indépendants les uns des autres ? Un pays est-il visé plus qu'un autre ? Les trois Etats les plus touchés au Moyen-Orient, à savoir Israël, le Liban et l'Iran, sont également les trois pays les plus touchés à l'échelle mondiale[82]. Or, plusieurs éléments permettent d'affirmer que la République islamique est la cible privilégiée de ces attaques cybernétiques. Pourquoi l'Iran plus qu'Israël et le Liban ? Selon David Sanger, le Président George W. Bush aurait mis en place une opération baptisée *Olympic Games* afin d'attaquer le programme nucléaire iranien par le biais des moyens cybernétiques à la disposition des Etats-Unis[83]. David Sanger précise que ce programme a été conduit par les Américains en partenariat avec leur allié israélien. Les Etats-Unis et Israël disposent effectivement des connaissances, des moyens financiers et des capacités pour conduire cette opération. Ils ne sont cependant pas les seuls. Plusieurs articles parus dans *Forbes* pointent ainsi du doigt la Finlande et la Chine[84]. Si les arguments avancés dans ces analyses pour établir la responsabilité de ces deux pays dans la conception de *Stuxnet* se tiennent, ils ne sont par contre plus valables pour les autres malwares qui ont touché l'Iran. La Chine peut effectivement avoir des raisons de vouloir saboter le programme nucléaire de Téhéran mais son intérêt à espionner les circuits financiers empruntés par l'argent du Hezbollah reste limité. Or, *Stuxnet* et *Gauss* sont liés.

En effet, les sociétés de sécurité informatique ont démontré que *Stuxnet* et *Duqu* sont basés sur le même système de programmation. Appelé par Kaspersky « *Tilded Platform* », cet élément permet donc de faire le lien entre les créateurs de ces deux malwares. Ils ont également montré que *Gauss* et *MiniFlame* découlent du même virus, à savoir *Flame*, et que là aussi leur système de programmation était identique entre eux. C'est pour cette raison que la plupart des analystes considéraient que ces deux familles de virus étaient l'œuvre d'équipes séparées n'ayant probablement pas de lien entre elles. Or, les équipes de recherche de Kaspersky ont découvert un module en étudiant *Flame* qui existe aussi dans *Stuxnet*. Ce module, appelé « ressource 207 » et qui permet la propagation de ces

[81] Dans le premier chapitre de cette étude, nous avons abordé les stratégies des Etats et leurs capacités dans le domaine cybernétique. Nous ne reviendrons donc pas en détail sur l'aspect opportunité.

[82] L'annexe 2 de cette étude (p. 50) est constituée de deux cartes qui détaillent, de manière différente, la répartition par pays des différents virus informatiques détectés au Moyen-Orient. Israël, le Liban et l'Iran apparaissent clairement comme les trois Etats les plus touchés dans la région.

[83] David E. Sanger, « Obama order sped up wave of Cyberattacks on Iran », New York Times, 1 juin 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

[84] Voir notamment Jeffrey Carr, « The New York Times fails to deliver Stuxnet's creators », 17 janvier 2011, Forbes, http://www.forbes.com/sites/jeffreycarr/2011/01/17/the-new-york-times-fails-to-deliver-stuxnets-creators/ qui est une réponse à un article du New York Times publié le 15 janvier 2011 et qui soulignait déjà les responsabilités d'Israël et des Etats-Unis. Voir aussi un article plus ancien dans lequel Jeffrey Carr détaille sa théorie, « Stuxnet's Finnish-Chinese Connection », 14 décembre 2010, Forbes, http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/

deux virus *via* des clés USB, est en tous points semblables dans les deux virus[85]. Il a été découvert dans la version 2009 de *Stuxnet* mais pas dans celle de 2010. Le module 207 permet donc d'affirmer que non seulement les deux projets sont liés mais que les équipes responsables de *Stuxnet/Duqu* ont également coopéré avec celles de *Flame/Gauss/MiniFlame* jusqu'en 2009. Le début de cette collaboration est difficile à dater. Les estimations du nombre d'années durant lesquelles *Stuxnet* et *Flame* ont été « actifs » varient entre 5 et 8 ans, soit une période s'étalant entre 2005 et 2008. Or, les plus anciens protocoles de *MiniFlame* connus à ce jour datent de 2007. Si on ajoute à cela le temps de conception, très difficile à estimer puisqu'il faut compter le temps de programmation et le temps de collecter les renseignements nécessaires, nous pouvons supposer que la décision de monter ces deux projets remonte au maximum à la première moitié des années 2000. C'est à ce moment-là que sont découverts deux sites nucléaires secrets en Iran.

Le programme nucléaire de Téhéran n'est toutefois pas la cible unique de ces attaques cybernétiques. C'est effectivement l'ensemble des activités iraniennes qui le sont. Si *Flame* montrait un intérêt particulier pour les PDF, les fichiers Microsoft Office et AutoCAD, laissant entendre qu'il ciblait le secteur industriel des pays où il a été découvert et donc notamment leurs infrastructures critiques, il n'en reste pas moins que son objectif était de récolter de l'information de masse. Or, outre Israël, *Flame* a surtout touché l'Iran, le Soudan et dans une moindre mesure les Territoires palestiniens et le Liban c'est-à-dire des territoires accusés par les autorités israéliennes de mener des activités hostiles à son égard. Le Soudan, qui a été bombardé par l'aviation israélienne en octobre 2012, sert de base logistique au trafic d'arme entre l'Iran et la Bande de Gaza. L'aide militaire iranienne arrive effectivement au Soudan par voie maritime, passe ensuite en Egypte par voie terrestre puis elle est transférait aux différents mouvements palestiniens *via* les tunnels creusés entre la péninsule du Sinaï et la Bande de Gaza[86]. Ces activités sont-elles à l'origine de l'idée de créer *Flame* ? Il est difficile de le dire mais il est clair que la taille du virus et les nombreux modules qui le composent démontrent la variété de ses cibles et donc du renseignement récolté.

Gauss, lui, s'intéresse à l'aspect financier des activités du Hezbollah. Les Etats-Unis et Israël s'interrogent depuis de nombreuses années sur le circuit emprunté par l'argent du mouvement chiite. Le financement du Parti de Dieu découle effectivement de l'aide iranienne mais aussi d'activités illicites, comme le trafic de drogue, menées par le Hezbollah en Amérique latine et ailleurs dans le monde[87]. L'intérêt porté au mouvement libanais découle aussi de ses liens étroits avec l'Iran et des opérations qu'il a réalisées au profit de la République islamique. Le Hezbollah est ainsi impliqué dans plusieurs attentats contre des intérêts israéliens. Le 13 février 2012, par exemple, une bombe visait simultanément un véhicule de l'ambassade israélienne en Géorgie et une voiture de l'ambassade israélienne en Inde. Le 18 juillet 2012, un attentat-suicide contre des touristes israéliens en Bulgarie faisait plusieurs victimes. Les Israéliens affirment avoir déjoué plusieurs tentatives d'attentats organisées ou commanditées par l'Iran dans une vingtaine de pays dont l'Azerbaïdjan, la

[85] Pour plus de détails sur le module 207 voir l'analyse de Kaspersky disponible en français : http://www.kaspersky.com/fr/about/news/virus/2012/Resource_207_une_etude_de_Kaspersky_Lab_met_en_evidence_le xistence_dun_lien_entre_les_developpeurs_de_Stuxnet_et_de_Flame

[86] Olivier Danino, « le Hamas et l'édification de l'Etat palestinien », Karthala, Paris, septembre 2009, 295 p.

[87] Matthew Levitt, « Hezbollah finances, funding the Party of God », The Washington Institute, février 2005, http://www.washingtoninstitute.org/policy-analysis/view/hezbollah-finances-funding-the-party-of-god

Thaïlande et Chypre. Les autorités de l'île ont d'ailleurs arrêté en juillet 2012 un jeune Libanais accusé de préparer un attentat contre des intérêts israéliens.

Ces évènements s'inscrivent dans un contexte particulièrement tendu entre Israël et l'Iran qui s'affrontent de manière indirecte depuis plusieurs années en raison du programme nucléaire de Téhéran. Ainsi, le 12 novembre 2011, une explosion détruisait des bâtiments situés sur une base militaire des Gardiens de la révolution et tuait plusieurs personnes, dont le général Hassan Moghadam, en charge du programme balistique de Téhéran. Le 11 janvier 2012, le professeur Mostapha Ahmadi Roshan, spécialiste nucléaire iranien, est assassiné à bord de sa voiture par une bombe magnétique. Ce ne sont que deux exemples des différents évènements mystérieux qui se sont passés en Iran ces dernières années. Si l'implication d'Israël est probable, elle n'a jamais été prouvée. Toutefois, il est clair que le programme nucléaire iranien est directement visé par ces attaques et il ne serait pas étonnant que le pays à l'origine de ces opérations utilisent aussi d'autres moyens, comme le cyber, pour arriver à ses fins.

La responsabilité des Etats-Unis et d'Israël dans la conception de ces différents malwares semble donc plus probable que celle de la Finlande et de la Chine. Et même si aucun de ces Etats n'est à l'origine de ces attaques cybernétiques, il n'en reste pas moins que l'Iran est clairement la cible d'une vaste opération d'espionnage et de sabotage qui vise non seulement son programme nucléaire mais aussi l'ensemble des ses activités. Téhéran n'est toutefois pas en reste. La République islamique aussi est soupçonnée d'avoir conçu deux virus informatiques : *Mahdi* et *Shamoon*. Ce dernier malware a frappé en août 2012 la compagnie saoudienne d'hydrocarbure, Aramco, et l'entreprise de gaz du Qatar, RasGas, le deuxième producteur de gaz naturel au monde. Les similitudes techniques trouvées par les sociétés de sécurité informatique entre *Wiper*, le malware qui a touché les installations d'hydrocarbure iraniennes, et *Shamoon* permettent de supposer que le premier a été pris pour modèle par les auteurs du second. Et a priori, personne n'est mieux placé que les Iraniens pour avoir accès aux données nécessaires.

De manière plus générale, le lien entre *Wiper* et *Shamoon* pose la question de la « prolifération cybernétique » c'est-à-dire de la multiplication de logiciels malveillants et de la possibilité pour un Etat, disposant du savoir-faire nécessaire, de s'inspirer d'un virus dont il a été victime pour en concevoir un autre. Au regard de ce qui a été fait pour *Shamoon*, il est tout à fait crédible d'imaginer que l'Iran se soit appuyé sur l'analyse des différents malwares qui l'ont pris pour cible afin de créer des virus pour attaquer Israël ou les pays de la péninsule arabique avec qui les relations sont également tendues. Il est d'ailleurs intéressant que le deuxième virus supposé d'origine iranienne, *Mahdi*, qui n'est relié à aucun malware particulier contrairement à *Shamoon*, ne soit pas un virus utilisé à des fins de sabotage mais à des fins d'espionnage. Il y a donc ici une sorte de mimétisme de la part de l'Iran qui imite, de manière toutefois bien moins sophistiquée, certains virus informatiques dont il a été la cible.

CONCLUSION

Les Etats du Moyen-Orient se sont tous appropriés le domaine cybernétique et l'ont tous placé au cœur de leur réflexion stratégique. Les Israéliens, qui s'intéressent à ce sujet depuis de nombreuses années, font clairement office de leader régional de par leur niveau technique, leurs connaissances et leurs compétences. Ils mènent une « stratégie institutionnelle » dans le sens où l'ensemble de leurs efforts en matière défensive et offensive reposent sur des institutions étatiques : l'INCB dépend du premier ministre, le ministère de la Défense a aussi son administration centrale en charge du cyber sans compter les unités militaires rattachées directement au commandement de Tsahal. Si l'impulsion vient de l'Etat aussi en Iran et en Syrie, ces deux pays ont toutefois fait le choix d'une « stratégie asymétrique » dans le domaine offensif c'est-à-dire qu'ils apportent leur soutien à des organisations non-étatiques qui agissent dans le cyberespace en fonction de leurs intérêts. Quant aux Etats de la péninsule arabique, leur stratégie est structurée essentiellement autour de CERTs dont la responsabilité première est d'assurer la protection de leurs systèmes d'information et de leurs infrastructures critiques. L'ouverture à Oman d'un centre aux compétences régionales est de ce point de vue intéressant car il traduit la volonté des pays de la péninsule de s'associer malgré les éventuelles tensions politiques qui peuvent exister entre certains d'entre eux. Enfin, la Turquie, qui s'est détournée de l'Europe pour recentrer sa diplomatie vers l'orient, n'a pas opéré le même virage dans le domaine du cyber. Pour le moment, le gouvernement turc privilégie les partenariats avec l'OTAN et semble se tourner vers ses nombreuses ressources, comme le Centre d'excellence de Tallinn[88].

En dehors de la Turquie, trois espaces stratégiques se dessinent donc au Moyen-Orient qui sont d'ailleurs trois espaces en opposition. Néanmoins, les rivalités entre Israël et la péninsule arabique sont minimes dans le domaine cybernétique. Si des hackers israéliens et arabes s'affrontent régulièrement, les Etats, eux, ne sont effectivement pas en opposition et restent même très prudents. Le gouvernement israélien n'a ainsi pas réagi lorsque la compagnie américaine de sécurité informatique, FireEye, a annoncé en décembre 2012 avoir repéré un malware qui transférait des données d'Israël vers le Koweït, alors qu'en janvier 2012, au moment où des hackers arabes et israéliens s'affrontaient par piratages interposés, les autorités israéliennes avaient annoncé qu'elles se réservaient le droit de riposter à ce type d'attaques par tous les moyens à leur disposition, dans le cyberespace et en dehors[89].

Il faut dire qu'Israël et les pays de la péninsule arabique ont le même allié dans le domaine cybernétique : les Etats-Unis. Le Qatar, l'Arabie Saoudite, les Emirats arabes unis sont effectivement très demandeurs d'outils spécialisés en sécurité informatique qu'ils se procurent principalement auprès d'entreprises américaines. Celles-ci ne sont toutefois pas les seules à s'impliquer auprès de ces Etats. Le gouvernement américain aussi assure une présence dans ces territoires comme l'illustre l'accord signé le 18 janvier 2013 entre le ministre de l'Intérieur saoudien, le prince Mohammed Ben

[88] Voir annexe 3 de cette étude (p. 51).

[89] Le virus supposé d'origine koweitienne se nomme Backdoor.L.V. Il récoltait des informations sur les utilisateurs des machines infectées (mots de passe, sites Internet consultés, fréquence d'utilisation de la webcam par exemple).

Naif, et la secrétaire à la Sécurité intérieure, Janet Napolitano. Ce texte porte sur un renforcement de la coopération cybernétique entre les deux pays et sur les moyens d'assurer une meilleure protection des infrastructures critiques du royaume saoudien. Israël et les Etats-Unis ont également signé plusieurs documents de ce type dont « l'accord de coopération scientifique et technologique en matière de sécurité intérieure » en mai 2008.

La ligne de fracture apparait ainsi plutôt entre Israël et la péninsule arabique, d'un côté, et le troisième espace stratégique composé de la Syrie et de l'Iran de l'autre. Les affrontements cybernétiques entre ces deux ensembles sont réguliers et d'intensité diverse. Des attaques par déni de service distribué, aux « défacements », en passant par des virus informatiques sophistiqués, les moyens utilisés sont effectivement nombreux. La guerre civile syrienne cristallise ces tensions. Israël est accusé par Bachar al-Assad de fournir des équipements de renseignement à l'opposition alors que l'Iran fait profiter son allié syrien de ses connaissances cybernétiques. L'implication de Téhéran dans les soulèvements qui secouent le monde arabe est souvent soulignée par certains Etats, notamment par ceux de la péninsule arabique. Le Hezbollah a ainsi été régulièrement accusé par le Bahreïn d'agir sur son territoire pour le compte de l'Iran et c'est d'ailleurs pour cette raison que l'archipel est devenu, en avril 2013, le premier pays arabe à placer le Parti de Dieu sur sa liste officielle des organisations terroristes.

La rivalité entre ces trois espaces stratégiques passe également par des groupes non-étatiques plus ou moins structurés. Leurs actions se limitent à des attaques au nom de tels ou tels camps. Ces opérations de nuisances tendent à se multiplier et sont même un élément à part entière des tensions de la région. Elles constituent le premier niveau d'utilisation offensif du cyber au Moyen-Orient et concernent principalement des vols données, des blocages et des modifications de contenus de sites Internet qui ont une valeur symbolique, comme ceux de la bourse d'Arabie Saoudite et des Emirats arabes unis ou celui du Mossad, le service de renseignement israélien. Ces groupes ne s'infiltrent pas dans les systèmes d'information de ces structures et leurs attaques ne remettent donc ni en question leur sécurité ni celle des Etats visés. Elles ont par contre un impact psychologique certain. C'est d'ailleurs leur principal intérêt. L'opération lancée par Anonymous en avril 2013 en est un exemple parfait. L'objectif officiel d'effacer Israël du cyberespace étant irréalisable au regard des moyens du mouvement, les piratages réalisés ont surtout touché la population qui est moins protégée que l'Etat et plus impressionnable.

La Syrie et l'Iran se sont alliés à certains de ces groupes de hackers qu'ils utilisent pour des opérations ponctuelles contre Israël et les pays de la péninsule arabique. L'Iran apporte également son soutien à des mouvements plus structurés qui expriment la volonté d'acquérir de réelles compétences cybernétiques. Il s'agit principalement du Hamas et du Hezbollah libanais. Si le premier est en cours d'acquisition de ces compétences, le second a fait preuve de son savoir-faire durant la dernière guerre qui l'a opposé à Israël. L'utilisation d'un drone par le Parti de Dieu en octobre 2012 démontre que le mouvement chiite a continué de progresser depuis 2006. La création d'une unité cyber au sein du Hezbollah illustre aussi bien l'intérêt porté à ce domaine par le mouvement chiite que sa volonté de l'intégrer complètement à ses capacités offensives. Pour le Hezbollah, comme pour le Hamas et pour Al-Qaïda, le cyber est en effet considéré comme un outil au potentiel destructeur élevé et dont l'utilisation dans le cadre d'un affrontement armé représente un véritable atout face à un adversaire militairement mieux équipé.

Par contre, pour de nombreux spécialistes, l'emploi de moyens cybernétiques à des fins uniquement terroristes reste peu probable. Pour eux, non seulement l'impact psychologique d'un attentat à la bombe reste plus fort que celui d'une attaque cybernétique mais le coût et les moyens nécessaires pour mettre au point un virus informatique reste plus onéreux que celui d'envoyer des hommes au suicide. Malgré cela, le lien entre *Wiper* et *Shamoon* démontre qu'un malware peut être créé par un Etat à partir d'un virus dont il a été victime et la collaboration entre l'Iran et le Hezbollah illustre la possibilité pour un mouvement non-étatique d'acquérir des compétences opérationnelles dans le cadre d'un transfert de connaissances. Il n'est donc pas totalement impossible qu'un groupe terroriste puisse accéder, avec l'aide d'un Etat, aux outils nécessaires pour lancer une attaque cybernétique massive. Certes, celle-ci ne provoquera pas directement de morts, et les images seront moins choquantes que celles de corps déchiquetés, mais l'impact psychologique sera obtenu grâce à la panique provoquée, surtout si elle est couplée à une opération terroriste d'envergure. Il suffit d'imaginer le résultat qu'aurait obtenu Al-Qaïda s'il avait lancé une attaque cybernétique sur les systèmes d'information des services de secours américains ou sur les infrastructures électriques de New York au moment des attentats du 11 septembre 2001.

Pour empêcher ce genre de situation de se produire, et pour se défendre plus généralement d'une attaque cybernétique de grande ampleur, la solution ne serait-elle pas, comme l'affirmait l'ancien commandant de l'armée de l'air israélienne, le général de division Eitan Ben Eliyahou, de créer des mécanismes de secours qui maintiendraient en état de marche les systèmes touchés par un virus informatique ? De cette manière, le fonctionnement des infrastructures critiques d'un Etat pourrait effectivement être assuré malgré les effets du malware. Ce qui suppose, pour Ben Eliyahou, que ce système de secours soit intégré au matériel informatique dès sa conception[90]. En tout cas, même si la possibilité d'une attaque terroriste par des moyens cybernétiques n'est pas considérée pour le moment crédible par les spécialistes, il ne faut pas oublier, comme le disait Denis Bauchard, qu'« au Moyen-Orient, seul l'imprévu est certain »[91].

[90] Israel Defense, « Fighting the next Cyber War », n°8, mai-juin 2012, pp. 68-70.

[91] Denis BAUCHARD, Israël 2007 : bilan et perspectives, Perspectives Moyen-Orient/Maghreb, Paris, IFRI, février 2007, p. 17.

ANNEXES

Annexe 1 : IDF in cyber space : Intelligence gathering and clandestine operations

IDF defines its activity in cyber space as a platform to improve operational effectiveness and defense. IDF has been relentlessly operating in the field

IDF Operations Department recently defined the essence of IDF cyber warfare, putting together instructions that define the military's operational methods in cyber space and clarify its goals in facing potential enemies. IDF Website exclusively reveals these instructions for the first time.

According to the document, cyber space is to be handled similarly to other battlefields on ground, at sea, in the air and in space. The IDF has been engaged in cyber activity consistently and relentlessly, gathering intelligence and defending its own cyber space. Additionally if necessary the cyber space will be used to execute attacks and intelligence operations.

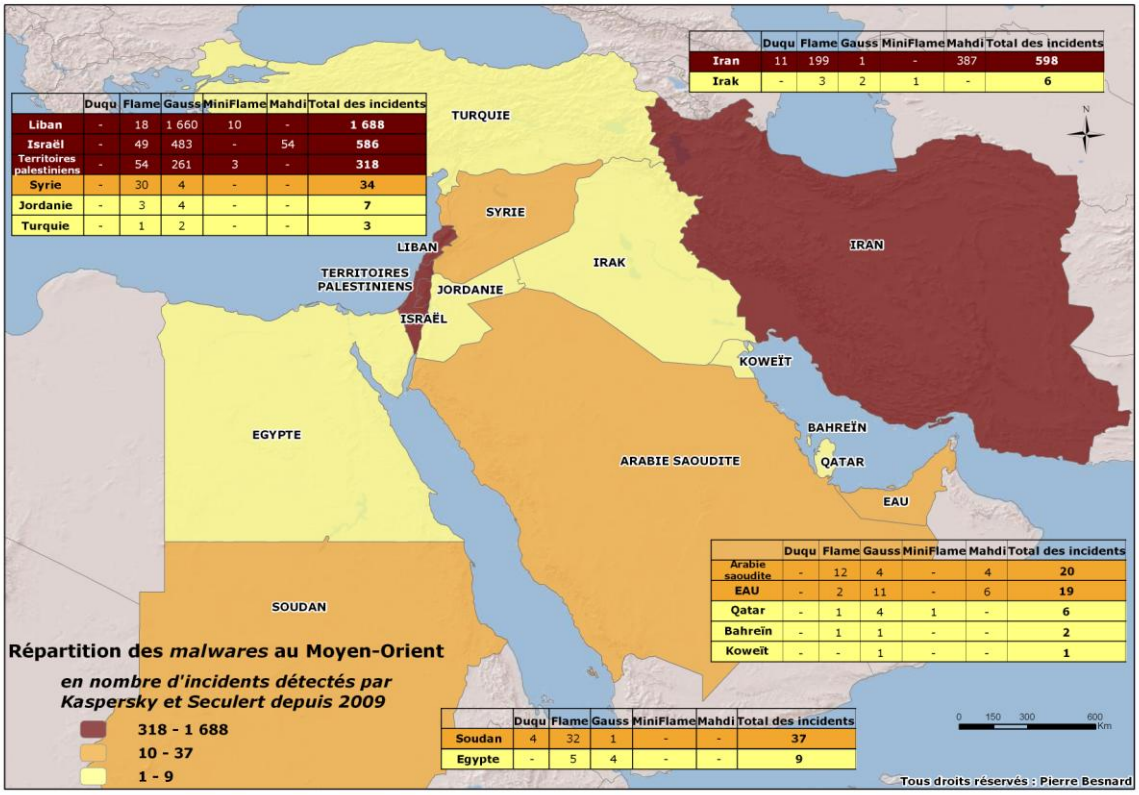
There are many, diverse, operational cyber warfare goals, including thwarting and disrupting enemy projects that attempt to limit operational freedom of both the IDF and the State of Israel, as well as incorporating cyber warfare activity in completing objectives at all fronts and in every kind of conflict. Moreover, it will be used to maintain Israel's quality and advantage over its enemies and prevent their growth and military capabilities, while limiting their operation in this field.

Additional goals defined by the document published by the Operations Department include creation of operational conditions that will assist in fulfilling IDF capabilities in combat as well as influence public opinion and raise awareness by advocating in the cyber space.

Overall cyber space will be used to improve the operational effectiveness of the IDF, both during war and peace time. This will be done through clandestine activity, while maintaining confidentiality and expertise.

Source : Rotem Pesso, « IDF in cyber space : Intelligence gathering and clandestine operations », 3 juin 2012, http://www.idf.il/1283-16122-en/Dover.aspx

Annexe 2 : Répartition des malwares au Moyen-Orient

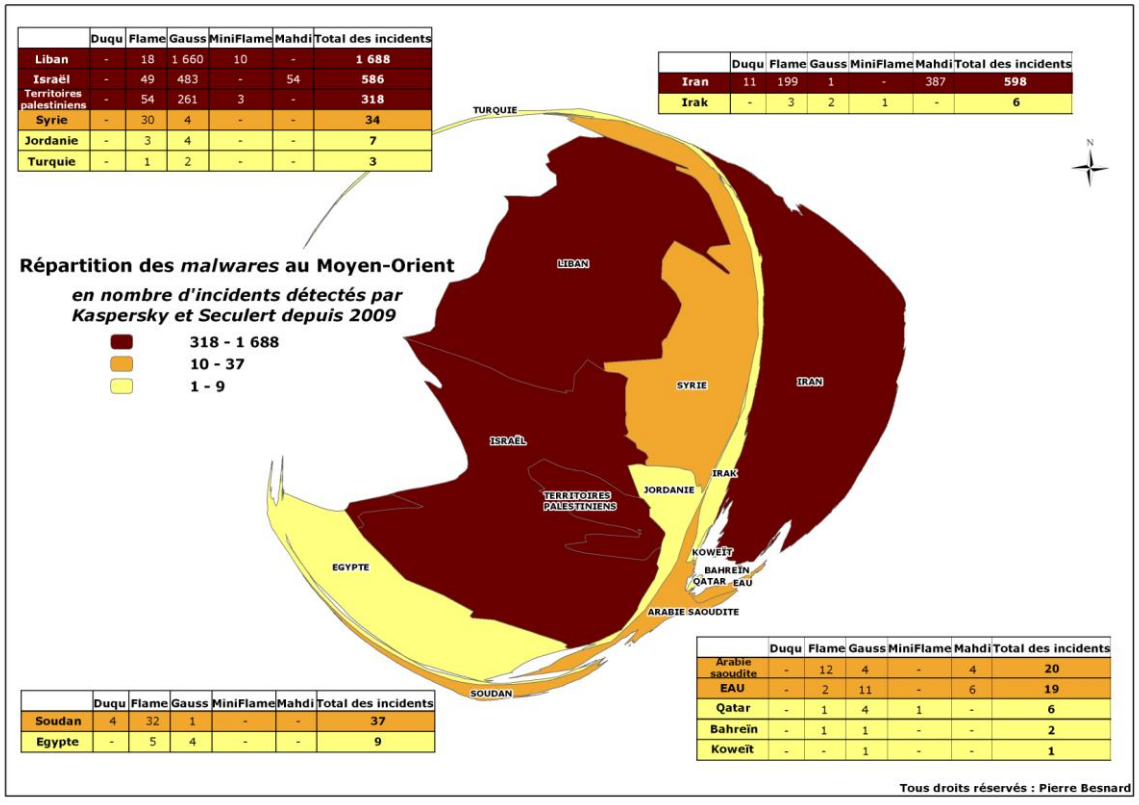


	Duqu	Flame	Gauss	MiniFlame	Mahdi	Total des incidents
Liban	-	18	1 660	10	-	1 688
Israël	-	49	483	-	54	586
Territoires palestiniens	-	54	261	3	-	318
Syrie	-	30	4	-	-	34
Jordanie	-	3	4	-	-	7
Turquie	-	1	2	-	-	3

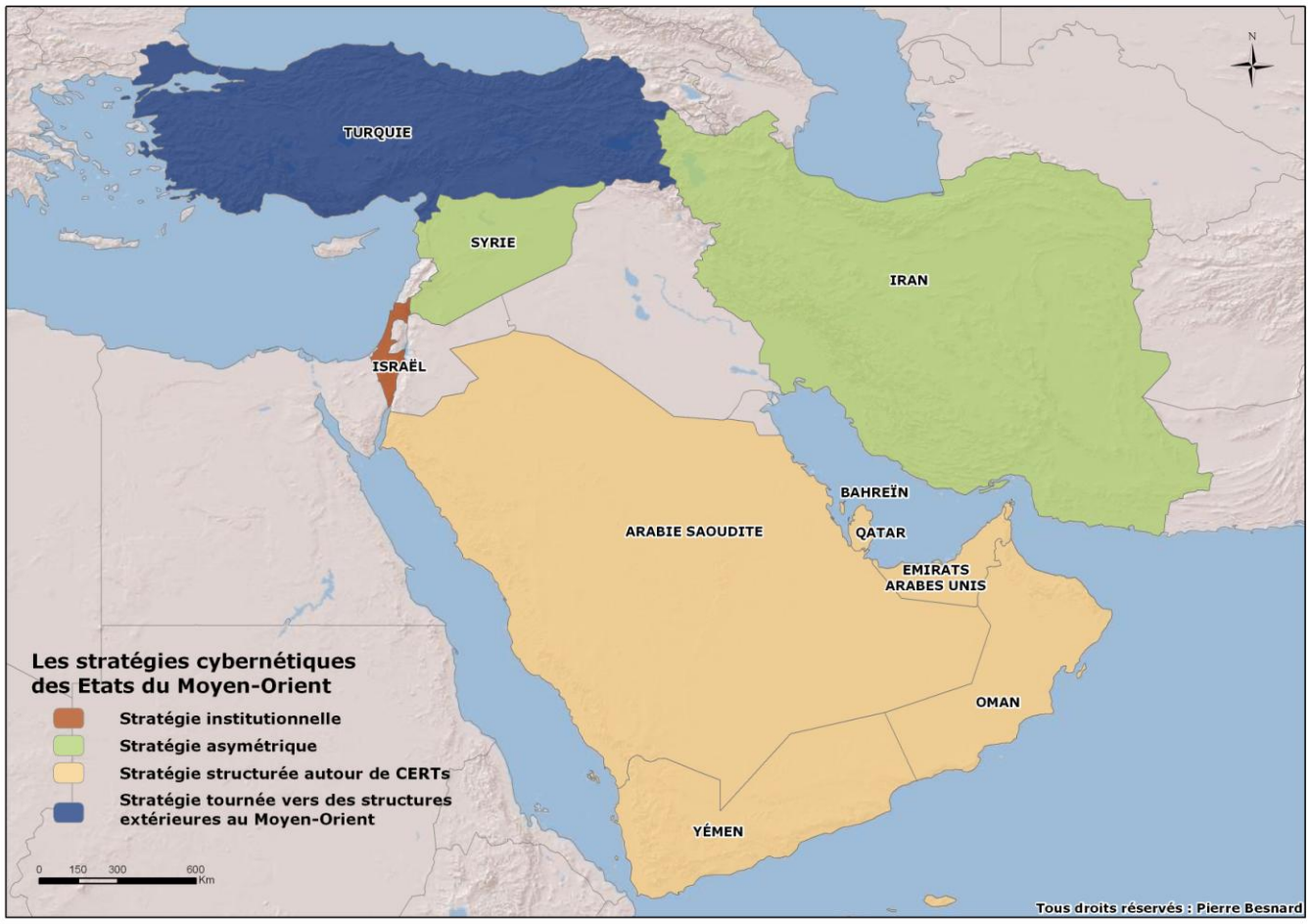
	Duqu	Flame	Gauss	MiniFlame	Mahdi	Total des incidents
Iran	11	199	1	-	387	598
Irak	-	3	2	1	-	6

	Duqu	Flame	Gauss	MiniFlame	Mahdi	Total des incidents
Arabie saoudite	-	12	4	-	4	20
EAU	-	2	11	-	6	19
Qatar	-	1	4	1	-	6
Bahreïn	-	1	1	-	-	2
Koweït	-	-	1	-	-	1

	Duqu	Flame	Gauss	MiniFlame	Mahdi	Total des incidents
Soudan	4	32	1	-	-	37
Egypte	-	5	4	-	-	9



Annexe 3 : Les stratégies cybernétiques des Etats du Moyen-Orient



BIBLIOGRAPHIE

Ouvrages et articles sur le Moyen-Orient :

- Anthony H. Cordesman, « Preliminary Lessons of the Israeli-Hezbollah War », Center for Strategic and International Studies (CSIS), 17 août 2006, Washington DC, http://csis.org/files/media/csis/pubs/060817_isr_hez_lessons.pdf
- Canadian Center for Intelligence and Security Studies, « La stratégie médiatique et de propagande d'Al-Qaïda », vol. 2, 2007, http://itac.gc.ca/pblctns/tc_prsnts/2007-2-fra.pdf
- Dalia Dassa Kaye, Alireza Nader, Parisa Roshan, « Israel and Iran, a dangerous rivalry », The RAND Corporation, 2011, 118 p.
- François Géré, « Iran, état de crise », Lignes de repères, Karthala, 2010, 250 p.
- Fred Burton et Scott Stewart, « Hezbollah : Signs of a Sophisticated Intelligence Apparatus », Stratfor, 12 décembre 2007, http://www.stratfor.com/weekly/hezbollah_signs_sophisticated_intelligence_apparatus
- International Crisis Group, « Yemen's Military-Security Reform : seeds of new conflict ? », Middle East Report, n° 139, 4 avril 2013.
- International Crisis Group, « Tentative Jihad : Syria's fundamentalist opposition », Middle East Report n° 131, 12 octobre 2012.
- International Crisis Group, « Popular Protest in North Africa and the Middle East : The Syrian Regime's slow-motion, suicide », Report n° 109, 13 juillet 2011.
- International Crisis Group, « Popular Protest in North Africa and the Middle East : The Syrian People's slow-motion revolution », Report n° 108, 6 juillet 2011.
- Jacqueline S. Kiel, « Hizbullah's Culture Wars, understanding Hizbullah through social movement theory and its media usage », Naval Postgraduate School, Californie, http://www.dtic.mil/dtic/tr/fulltext/u2/a496945.pdf.
- Jeremy M. Sharp et Christopher M. Blanchard, « Armed conflict in Syria : US and International response », CRS Report for Congress, 19 juillet 2012, http://www.fas.org/sgp/crs/mideast/RL33487.pdf
- Matthew Levitt : « Hezbollah : the global footprint of Lebanon's Party of God », George Tow University Press, 368 p.
- Matthew Levitt, « Hezbollah finances, funding the Party of God », The Washington Institute, février 2005, http://www.washingtoninstitute.org/policy-analysis/view/hezbollah-finances-funding-the-party-of-god
- Olivier Danino, « le Hamas et l'édification de l'Etat palestinien », Karthala, Paris, septembre 2009, 295 p.

- Pierre Razoux, « Israël frappe la Syrie : un raid mystérieux », *Politique étrangère*, n°1, 2008, IFRI, Armand Colin, Paris.

Ouvrages, articles et rapports sur le cyber :

- Alex Lukich, « The Iranian Cyber Army », Center for Strategic and International Studies (CSIS), 12 juillet 2011, http://csis.org/blog/iranian-cyber-army
- Ali Alkarni, « A media/terrorism model : the Saudi Experience », King Saud University, Riyad, 2008, http://faculty.ksu.edu.sa/alkarni/DocLib1/media%20terrorism%20model%20the%20saudi%20experience.pdf
- Brian Michael Jenkins, « Is Al-Qaeda's Internet Strategy working ? », Rand Corporation, décembre 2011, 7 p. http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT371.pdf
- Catherine A. Theohary et John Rollins, « Terrorist use of the Internet : Information operations in Cyberspace », CRS Report for Congress, 8 mars 2011, http://www.fas.org/sgp/crs/terror/R41674.pdf
- Céline Pigot et Alexandre Durand, « Nouvelles guerres de l'information, le cas de la Syrie », CEIS, les notes stratégiques, novembre 2012, http://www.ceis.eu/fr/actu/note-strategique-nouvelles-guerres-de-l-information-le-cas-de-la-syrie-celine-pigot-et
- Clay Wilson, « Computer attack and Cyberterrorism : Vulnerabilities and Policy issues for Congress », CRS Report for Congress, 1 avril 2005, http://fpc.state.gov/documents/organization/45184.pdf
- Clay Wilson, « Botnets, Cybercrime and Cyberterrorism : Vulnerabilities and Policy issues for Congress », CRS Report for Congress, 29 janvier 2008, http://www.fas.org/sgp/crs/terror/RL32114.pdf
- Eva Galperin et Morgan Marquis-Boire, « New malware targeting Syrian Activists uses BlackShades commercial trojan », Electronic Frontier Foundation, 12 juillet 2012, https://www.eff.org/deeplinks/2012/07/new-blackshades-malware
- Fondation of American Scientists, « Iraqi Insurgency Group utilizes Google Earth for attack planning », juillet 2006, http://www.fas.org/irp/dni/osc/osc071906.pdf
- Gary R. Bunt, « Islam in the Digital Age, E-Jihad, online Fatwas and Cyber Islamic Environments », Pluto Press, Londres, 2003, 238 p.
- Infowar Monitor, « Syrian Electronic Army disruptive attacks and hyped targets », 25 juin 2011, http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/
- Institute for Security Technology Studies (ISTS), « Examining the Cyber Capabilities of Islamic Terrorist Groups », Darthmouth College, 2003, http://www.ists.dartmouth.edu/docs/ITB_032004.pdf
- Jean Loup Samaan, « Mythes et réalités des cyberguerres », *Politique étrangère*, IFRI, n° 4, 2008, p. 830.

- Jeffrey Carr, « Inside Cyber Warfare », O'Reilly, 2e édition, décembre 2011.
- John Rollins et Clay Wilson, « Terrorist capabilities for cyberattack : Overview and Policy issues », CRS Report for Congress, 22 janvier 2007, http://www.fas.org/sgp/crs/terror/RL33123.pdf
- Laurent Bloch et Christophe Wolfhugel, « Sécurité informatique, principes et méthodes à l'usage des DSI, RSSI et administreurs », Eyrolles, 2009.
- Margaret Weiss, « Assad's Secretive Cyber Force », The Washington Institute, Policy Watch 1926, 12 avril 2012 http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFQQFjAA&url=http%3A%2F%2Fwww.washingtoninstitute.org%2Fpolicy-analysis%2Fpdf%2Fassads-secretive-cyber-force&ei=fk4iUMbsKsWt0QWy6IHYDA&usg=AFQjCNG2wOCnxPUBATRyapuRGHYExcwhJQ&sig2=5_yVsg9B0lDHRqJ5sH9qvQ
- Marvin Kalb et Carol Saivetz, « The Israeli-Hezbollah war of 2006 : The Media as a weapon in Asymmetrical Conflict », Harvard's Kennedy School of Government, 2007, http://www.brookings.edu/~/media/events/2007/2/17islamic%20world/2007islamforum_israel%20hezb%20war
- Martin C. Libicki, « The Strategic Uses of Ambiguity in Cyberspace », Military and Strategic Affairs, vol. 3, n°3, décembre 2011, http://cdn.www.inss.org.il.reblazecdn.net/upload/(FILE)1333532281.pdf
- Maura Conway, « Cybercortical Warfare : the case of Hezbollah.org », Trinity College, Dublin, 2003, http://www2.scedu.unibo.it/roversi/SocioNet/Conway.pdf
- Michele Zanini, « Middle Eastern Terrorism and Netwar », Rand, Santa Monica, 1999, http://www.ou.edu/ap/lis5703/whatisresearch/terrorism.pdf
- Morgan Marquis-Boire et Seth Hardy, « Syrian Activists Targeted with BlackShades Spy Software », juin 2012, https://citizenlab.org/wp-content/uploads/2012/08/06-2012-syrianactiviststargeted.pdf
- Richard A. Clarke et Robert K. Knake, « Cyber War, the next Threat to National Security and what to do about it », Harper Collins, New York, 2010.
- Sabrine Saad, Stéphane B. Bazan, Christophe Varin, « Asymmetric Cyber-warfare between Israel and Hezbollah : the Web as a new strategic battlefield », Université Saint-Joseph de Beyrouth, http://www.websci11.org/fileadmin/websci/Posters/96_paper.pdf
- Shmuel Even et David Siman-Tov, « Cyber Warfare : Concepts and Strategic Trends », Institute for National Security Studies, memorandum 117, mai 2012, http://cdn.www.inss.org.il.reblazecdn.net/upload/(FILE)1337837176.pdf
- Thomas Rid et Marc Hecker, « les armées doivent-elles craindre les réseaux sociaux », dans Politique étrangère, « l'Internet outil de puissance », IFRI, n°2, 2012, pp. 317-328.
- Thomas Rid et Marc Hecker, « War 2.0 : Irregular Warfare in the Information Age », Praeger Security International, London, 2009, 280 p.

- Yoram Schweitzer, Gabi Siboni et Einav Yogev, « Cyberspace and Terrorist Organisations », Military and Strategic Affairs, vol. 3, n°3, décembre 2011, http://cdn.www.inss.org.il.reblazecdn.net/upload/(FILE)1333532806.pdf

Articles de presse sur le cyber :

- Al Jazeera, « Iran to launch giant domestic Intranet », 24 septembre 2012, http://www.aljazeera.com/news/middleeast/2012/09/201292471215311826.html
- Hossein Bastani, « Structure of Iran's Cyber Warfare », BBC Persian, http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf
- David Eshel, « Hezbollah intelligence War », http://defense-update.com/analysis/lebanon_war_1.htm
- David E. Sanger, « Obama order sped up wave of Cyberattacks on Iran », New York Times, 1 juin 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0
- David Millian, « Médias sociaux et printemps arabes : plongée dans le 2.0 au cœur de la révolution lybienne », http://comfluences.net/2012/05/31/medias-sociaux-et-printemps-arabe-plongee-au/
- Fars News Agency, « Iran Boosting Electronic War Capabilities due to Nature of Threats », 1er octobre 2012, http://english.farsnews.com/newstext.php?nn=9106243312
- Ilana Curiel, « Deputy FM threatens forceful response to cyber attacks », Ynet, 7 janvier 2012, http://www.ynetnews.com/articles/0,7340,L-4172329,00.html
- Jack Cloherty, « Virtual Terrorism : Al Qaeda Video calls for Electronic Jihad », ABC News, Mai 2012, http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UVLyGxc2YWs
- Jay Newton-Small, « Hillary's Little Startup: How the U.S. Is Using Technology to Aid Syria's Rebels », Time World, 13 juin 2012**,** http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/
- Jeffrey Carr, « The New York Times fails to deliver Stuxnet's creators », 17 janvier 2011, Forbes, http://www.forbes.com/sites/jeffreycarr/2011/01/17/the-new-york-times-fails-to-deliver-stuxnets-creators/
- Jeffrey Carr détaille sa théorie, « Stuxnet's Finnish-Chinese Connection », 14 décembre 2010, Forbes, http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/
- Khashayar Nouri, « Cyber Wars in Iran », Mianeh, 22 juillet 2010, http://mianeh.net/article/cyber-wars-iran
- Pierre Alonso, « La Syrie, coupure net », OWNI, 7 juin 2011, http://owni.fr/2011/06/07/la-syrie-coupure-net/
- Roi Kais, « Kuwaiti imam : cyber jihad effective », Ynet, 18 janvier 2012, http://www.ynetnews.com/articles/0,7340,L-4177268,00.html

- Vita BEKKER, Barak admits Israel's cyberwar activity, Financial Times, 6 juin 2012, http://www.ft.com/cms/s/0/43f199f2-afec-11e1-b737-00144feabdc0.html
- Von Sarah Stricker, « Online-Spionage : Die schöne Facebook-Freundin der Elitesoldaten », Der Spiegel, Mai 2010, http://www.spiegel.de/politik/ausland/online-spionage-die-schoene-facebook-freundin-der-elitesoldaten-a-694582.html
- William Saffire, « The Farewell Dossier », The New York Times, 2 février 2004, http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html
- Yaakov Katz, « Army seals off Hizbullah stronghold of Bont Jbail », The Jerusalem Post, http://www.jpost.com/LandedPages/PrintArticle.aspx?id=29385

Etudes sur les virus informatiques :

- Kaspersky, « Malware Evolution », Security Bulletin 2012, http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons
- Kaspersky, « Cyber Weapons », Security Bulletin 2012, http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons
- Kaspersky, « MiniFlame a.k.a SPE : Elvis and his friends », Securelist, 17 juillet 2012, http://www.securelist.com/en/analysis/204792247/miniFlame_aka_SPE_Elvis_and_his_friends
- Kaspersky, « The Madi Campaign – Part I », Securelist, 17 juillet 2012, http://www.securelist.com/en/blog/208193677/The_Madi_Campaign_Part_I
- Kaspersky, « Gauss : Abnormal Distribution », Securelist, 9 août 2012, http://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf
- Kaspersky, « Gauss : Nation-state cyber-surveillance meets banking Trojan », Securelist, 9 août 2012, http://www.securelist.com/en/blog/208193767/Gauss_Nation_state_cyber_surveillance_meets_banking_Trojan
- Kaspersky, « What was that Wiper thing ? », Securelist, 29 août 2012, https://www.securelist.com/en/blog/208193808/What_was_that_Wiper_thing
- Kaspersky, « Shamoon the Wiper, Copycats at Work », Securelist, 16 août 2012, http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work
- Kaspersky, « Back to Stuxnet : the missing link », Securelist, 11 juin 2012, https://www.securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link
- Kaspersky, « Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected », 11 juin 2012, http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected
- Myriam Dunn Cavelty, « Unraveling the Stuxnet effect : Of much and little change in the cyber threats debate », Military and Strategic Affairs, Vol. 3, n°3, décembre 2011, pp.11-19

- Paul K. Kerr, John Rollins et Catherine A. Theohary, « The Stuxnet Computer Worm : Harbinger of an Emerging Warfare Capability », CRS Report for Congress, 9 décembre 2010, 9 p

- Paul Mueller et Babak Yadegari, « The Stuxnet Worm », Département des sciences de l'informatique, Université de l'Arizona, http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

- Seculert, « Shamoon, a two-stage targeted attack », 16 août 2012, http://blog.seculert.com/2012/08/shamoon-two-stage-targeted-attack.html

- Symantec, « W32.Stuxnet », http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

- Université de technologie et d'économie de Budapest et le laboratoire de cryptographie et de sécurité système (CrysSys Lab), « SkyWiper (a.k.a Flame a.k.a Flamer) : A complex malware for targeted attacks », 31 mai 2012, http://www.crysys.hu/skywiper/skywiper.pdf

- Université de technologie et d'économie de Budapest et le laboratoire de cryptographie et de sécurité système (CrysSys Lab), « Duqu : A Stuxnet-like malware found in the wild », 14 octobre 2011, http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

Documents officiels :

- Agence nationale de la sécurité des systèmes d'information (ANSSI), « Défense et sécurité des systèmes d'information, stratégie de la France », février 2011.

- Alexander S. Adjemov et al., « International Information Security : Problems and Decisions », éd. Komov SA, Moscou, 2011.

- Deparment of Defense, « Dictionary of Military and Associated Terms », 15 décembre 2012.

- Frank J. Cilluffo, « The Iranian Cyber Threat to the United States », US House of representatives, Committee on Homeland Security, Homeland Security Policy Institute, 26 avril 2012.

- ICTQatar, « Controls for the Security of Critical Industrial Automation and Control Systems Guidelines », http://www.ictqatar.qa/sites/default/files/documents/Controls_English_Version_0.pdf

- Ministry of Communication and Information Technology, « Developing National Information Security Strategy for the Kingdom of Saudi Arabia », National Information Security Strategy, draft 7, http://www.mcit.gov.sa/NR/rdonlyres/514E7B51-5710-46D9-9EC5-2D78BC2E1219/0/NISS_Draft_7_EN.pdf

- Rotem Pesso, « IDF in cyber space : Intelligence gathering and clandestine operations », 3 juin 2012, http://www.idf.il/1283-16122-en/Dover.aspx

TABLE DES MATIERES