Observatoire du Monde Cybernétique
Trimestriel

Mars 2013

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 la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

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

Sommaire

1. Industrie américaine de la cybersécurité - Etat des lieux

Le marché mondial de la cybersécurité devrait atteindre 68,3 milliards de dollars en 2013[1]. Sans surprise, les Etats-Unis constituent le marché le plus dynamique. On y observe même un engouement certain pour le secteur : les valeurs de l'industrie cyber sécuritaire sont chaudement recommandées par les analystes, les levées de fond se multiplient, les introductions en bourse sont fébrilement attendues et remportent un vif succès… Quelles sont les raisons profondes de cette dynamique ? Ses bases sont-elles solides ? S'inscrit-elle dans le long terme ? Existe-il un risque de bulle à l'image de la bulle dot.com de la fin des années 90 et début 2000 ?

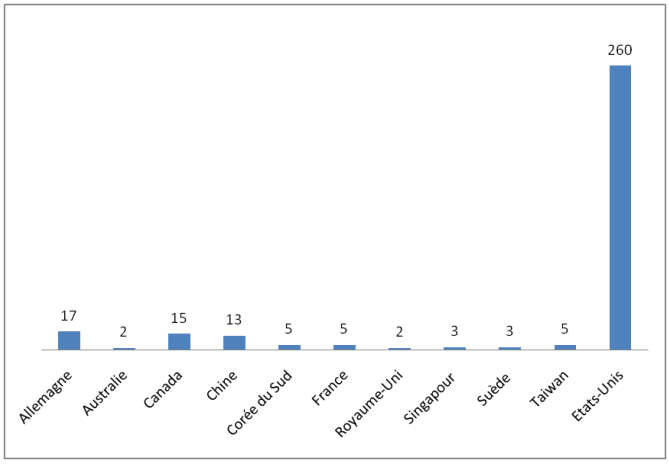
1.1 Un secteur en pleine effervescence

Avec 24 000 participants et 360 exposants, la conférence RSA qui s'est tenue fin février 2013 aux Etats-Unis n'avait jamais remporté un tel succès. D'un point de vue quantitatif, l'événement a compté 20 % d'exposants en plus par rapport à l'année dernière, et ce malgré la centaine de fusion-acquisitions observées en 2012 dans le secteur des technologies de l'information. C'est aussi la première fois que les sociétés étrangères étaient aussi présentes, ce qui témoigne du caractère global du marché de la cybersécurité. Si les Etats-Unis se sont logiquement taillé la part du lion avec 260 exposants, on comptait en effet 17 exposants allemands, 15 canadiens et 13 chinois. Même Huawei, qui avait fait l'objet en octobre dernier d'un rapport du Congrès américain soulignant le danger que l'entreprise représentait pour la sécurité nationale, avait fait le déplacement. Arrivée en 5ème position, la France comptait pour sa part 5 exposants[2], ex aequo avec Taïwan ou la Corée du Sud.

[1] http://www.visiongain.com/Report/951/Global-Cyber-Security-Market-2013-2023

[2] 6vind, Groupe Eleven, Oberthur Technologies, Qosmos, Thales e-Security

Répartition des exposants à la RSA Conférence par nationalité[3]



Au-delà des aspects quantitatifs, c'est l'effervescence du secteur aux Etats-Unis qui a frappé la plupart des observateurs. Un tiers des exposants américains étaient en effet des PME au chiffre d'affaires inférieur à 10 millions d'euros, parmi lesquelles nombre de toutes jeunes start-up installées sur les « nouveaux » créneaux de la cybersécurité : lutte contre les APT, « big data » (en lien direct avec le thème de la conférence qui était : « security is knowledge. Mastering data. Securing the world ») ou bien encore sécurisation du cloud computing et des équipements mobiles.

15 start-up américaines en pointe dans le domaine de la cybersécurité[4]

Nom	Site internet	Description
Appthority	https://www.appthority.com/	Propose une plateforme cloud permettant de vérifier si une application mobile est sûre ou non.
Marble Cloud	http://marblecloud.com/	Solution de sécurisation du BYOD.
AnchorFree	http://www.anchorfree.com/	Solution de VPN sécurisé (Hotspot Shield) offrant une connexion anonyme et sécurisée à Internet. Goldman Sachs a injecté 52 millions de dollars dans l'entreprise en 2012. La plateforme a notamment été utilisée pendant

[3] La nationalité des exposants, entreprise ou organisation, a été identifiée à partir du siège de l'entité. Plusieurs sociétés d'origine israélienne comme CheckPoint ou Cyber-Ark sont ici considérées comme américaines ayant localisé leurs sièges sociaux aux Etats-Unis et étant cotées dans ce pays.

[4] Source : http://www.businessinsider.com/15-most-important-security-startups-2013-1?op=1 et CEIS

		par les opposants lors des révoltes du Printemps arabe.
Wickr	https://www.mywickr.com/en/index.php	Solution de chiffrement et d'anonymisation des échanges pour plateformes mobiles.
Impermium	http://www.impermium.com/	Solution d'authentification à plusieurs niveaux basée sur une analyse de risque temps réel menée à partir du profil de la personne qui se connecte (adresse IP, comportements, équipements).
Victrio	http://www.victrio.com/	Système anti-fraude temps réel basé sur une technologie de prise d'empreinte vocale.
Shape Security	http://www.shapesecurity.com/	Protection des sites web et e-commerce. L'entreprise a levé 20 millions de dollars récemment, notamment auprès de Venrock et Kleiner Perkins. L'entreprise a été confondé pa Sumit Agarwal, ancien responsable de l'unité mobile de Google.
41st Parameter	http://www.the41.com/	Solution d'authentification basée sur un mécanisme de prise d'empreinte de l'ordinateur se connectant. Fondée par Ori Eisen, ancien directeur fraude d'American Express.
Tenable Network Security	http://www.tenable.com/	Son produit phare est Nessus, logiciel d'analyse des vulnérabilités. A signé un important contrat avec le DoD américain. Accel a récemment injecté 50 millions dans l'entreprise.
CrowdStrike	http://www.crowdstrike.com/	Solution de lutte informatique défensive dynamique basée sur l'analyse des tactiques, techniques et méthodes utilisées par les hackers. Fondé par Goerge Klutz, ancien CTO de McAfee.
FireEye	http://www.fireeye.com/	Solutions de protection contre les APT intégrant firewall, IPS, antivirus et passerelle. FireEye est l'une des start up phare du marché

		et son introduction en bourse est fébrilement attendue.
Co3 Systems	https://www.co3sys.com/	Solutions de gestion d'incident et compliance.
Bromium	http://www.bromium.com/	Technologie de micro-virtualisation permettant de lancer des applications de façon étanche. Fondé par Simon Crosby, fondateur de XenSource.
CipherCloud	http://www.ciphercloud.com/	Chiffrement en temps réel des données avant envoi dans le cloud. Fondée par Pravin Kothari, ancien patron d'ArcSight. Andreessen Horowitz a récemment injecté 30 millions de dollars dans l'entreprise.
ThreatMetrix	http://threatmetrix.com/	Solution d'analyse de données sécurité et de lutte anti-fraude.

1.2 Un volontarisme politique sans faille

1.2.1 Au niveau fédéral

Le dynamisme de l'industrie de cybersécurité américaine s'explique très largement par le volontarisme du gouvernement américain. Au plan politique et idéologique, il martèle depuis des années que la cybersécurité est une exigence stratégique face à la montée des menaces dans le cyberespace et contribue en cela à façonner l'opinion publique américaine, voire mondiale. Derniers épisodes en date : *l'executive order* de janvier 2013 sur la cybersécurité des infrastructures critiques, le rapport de la société Mandiant soulignant la responsabilité du gouvernement chinois dans les attaques informatiques visant les Etats-Unis et les discours martiaux de nombreux responsables politiques, tant démocrates que républicains. Lors de la conférence RSA 2013, Condoleeza Rice (qui pourrait briguer l'investiture républicaine lors de la prochaine présidentielle) déclarait ainsi qu'elle considérait que l'effort du pays pour se préparer à la menace « cyber » était du même niveau que celui fait après le 11 septembre.

Au plan économique enfin, le gouvernement s'est donné les moyens de sa politique. Dans un contexte budgétaire très contraint, en particulier pour la défense, les budgets affectés à la

cybersécurité vont continuer à croître. Le marché fédéral de cybersécurité est ainsi évalué à 65,5 milliards de dollars sur les 6 prochaines années (2013-2018), avec une progression annuelle de 6,2 % environ[5]. Le regroupement sur le même site de la NSA (qui possédait un vaste stand à la conférence RSA 2013), de la DISA et du Cyber Command constitue ainsi un véritable pôle d'attraction pour les acteurs privés, jusqu'à former une nouvelle « Silicon Valley de la cybersécurité ». Le passage du cyber command de 900 personnes à 4 900 personnes, civils ou militaires, entraînera en effet nécessairement de l'externalisation et des contrats de prestations pour le secteur privé. La NSA est ainsi qualifiée de « acquisition hot spot »[6] : toute société disposant de contrats avec elle voit sa valeur s'envoler. De fait, les acquisitions de « NSA contractors » se sont multipliées depuis la création du Cyber Command.

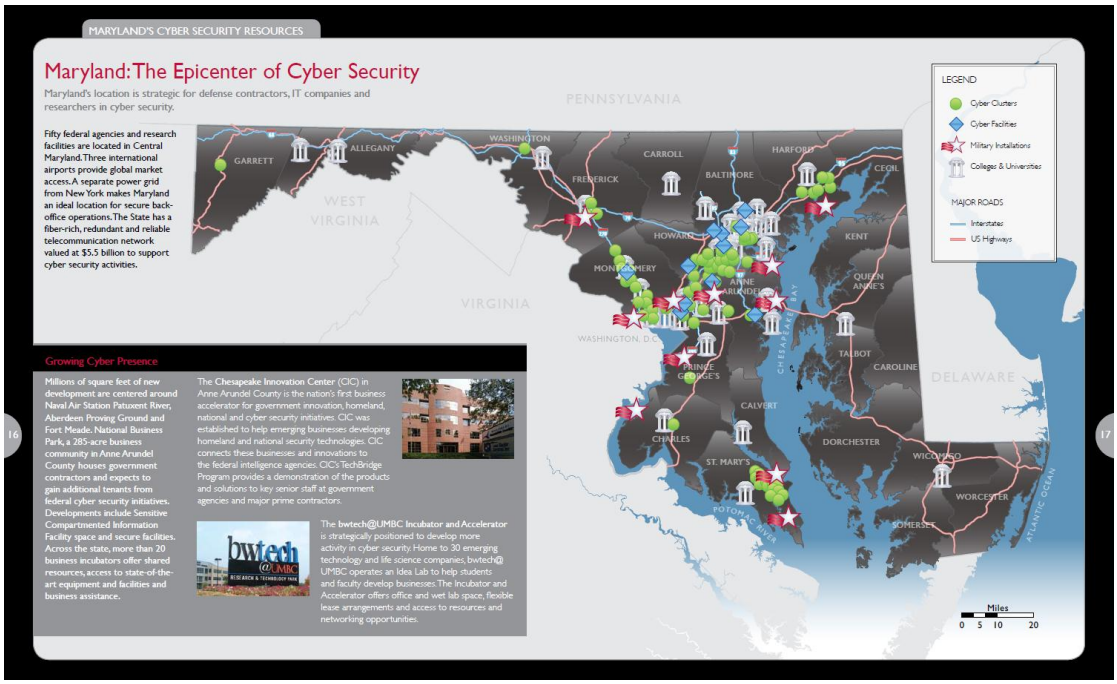
1.2.2 Au plan local

Grâce à la présence de la NSA, du Cyber Command, de la DISA mais aussi du NIST ou de l'IARPA, le Maryland, s'est autoproclamé « US hub for the cybersecurity industry » et « épicentre de la sécurité de l'information et de l'innovation »[7]. Les autorités ont ainsi créé un site Internet (http://www.cybermarylandmap.com/) listant l'ensemble des acteurs du secteur, entreprises, universités et centres de recherche. On dénombre ainsi pas moins de 52 entreprises intervenant dans le domaine de la cybersécurité, soit au total 60 000 salariés dans le domaine.

Soucieux de dynamiser encore la filière, le gouvernement de l'Etat du Maryland examine en ce moment la possibilité de créer un avantage fiscal pour les particuliers et entreprises qui investiraient jusqu'à 500 000 dollars dans une société de cybersécurité, sur le modèle du dispositif existant pour les biotechnologies. Des incubateurs spécialisés ont également vu le jour comme le Research & Technology Park adjacent à l'Université du Maryland[8] qui propose un Cyber Incubator pouvant soutenir les « jeunes pousses » lors du lancement de leurs activités. Un partenariat a été mis en place avec Northrop Grumann pour favoriser le développement et la commercialisation des solutions innovantes développées par ces entreprises. Dernier exemple d'action engagée par l'Etat du Maryland : le développement des activités de R&D autour du nouveau Cyber Center of Excellence du NIST.

[5] http://www.marketresearchmedia.com/?p=206
[6] http://www.aronsoncapitalpartners.com/blog/?cat=23
[7] Voir la plaquette de l'Etat du Maryland intitulée « Cybermaryland » : http://www.choosemaryland.org/aboutdbed/documents/finalcyberreport.pdf
[8] http://www.bwtechumbc.com/

Extraits de la plaquette « CyberMaryland »



Après le Maryland, la Virginie voisine n'est pas en reste. Une publication récente[9] décrit l'écosystème local en matière de cybersécurité. On relève la présence d'environ 300 entreprises dans le domaine, dont le Center for Cyber Innovation de Deloitte situé à Arlington. Sans oublier le riche tissu universitaire de cet Etat. Les universités George Mason, James Madison, Norfolk State et Virginia Tech ont ainsi été désignés comme centre d'excellence en R&D et en cybersécurité par la NSA et le DHS (Information Assurance Education).

1.3 Des capitaux-risqueurs très actifs

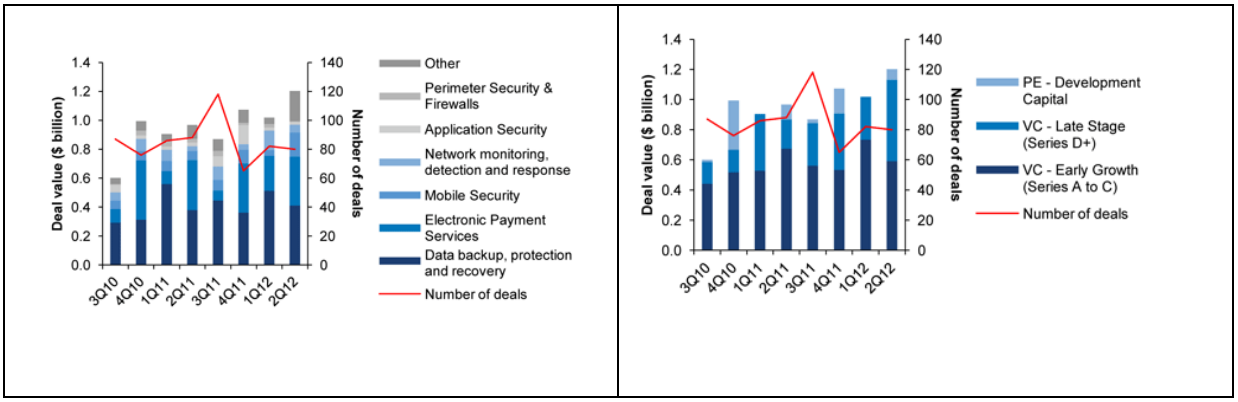
Le dynamisme du secteur de la cybersécurité s'explique sans aucun doute d'abord par le soutien très actif des capitaux-risqueurs et fonds d'investissement, au premier rang desquels les fonds Sequoia ou Accel Partners qui ont investi à eux deux dans une cinquantaine d'entreprises depuis 2010. Au total, en 2011, les fonds d'investissements ont ainsi injecté 935 millions de dollars dans le domaine, soit le double du montant investi en 2010[10], avec un focus particulier dans les domaines de la sécurité

[9] Virginia's Innovation Ecosystem : the trusted leader in growing cyber security solutions

[10] Rapport MoneyTree, PwC, National Venture Association, Thomson Reuters.

mobile, de l'authentification, de la détection d'intrusion et du big data, ce qui montre un changement de priorité par rapport aux années précédentes. Point clé, ces investissements concernent surtout les premiers stades de développement des entreprises, de l'amorçage aux phases de développement initiales.

Analyse des investissements par domaine et par stade de développement[11]



Principaux fonds par nombre de deals dans le domaine de la cybersécurité entre avril 2010 et mars 2012[12]

Investisseur	Nombre de deals	Principaux investissements (non exhaustif)
Sequoia Capital	28	Click Security, Bit9. Anciennes participations : Palo Alto networks.
Accel Partners	25	Imperva, Tenable Network Security, Lookout (blocage de malware et spyware sur appareils mobiles)
Intel Capital Corp	24	Solera Networks (détection d'intrusion)
Lightspeed Venture Partners	20	Click Security

[11] http://www.cybersecurityfinanceforum.com/Analysis

[12] Source : http://www.raymondjames.com/ecm/library/pdfs/1205_global_security_finance.pdf et CEIS

Ignition Partners	20	Morta Security, Docusign (signature électronique), Symplified
New Enterprise Associates	19	CloudFlare, Force10Networks, Netcitadel (cloud)
Greylock partners	17	Imperva, Morta Security
Benchmark Capital	16	Juniper Networks
Index Ventures	14	CipherCloud
Khosla Venture	14	Cylance,
Battery ventures	14	VibeSec
North Bridge Venture Partners	14	OneID
Kleiner Perkins Caufield & Byers	13	Bit9, Shape Security, Mendiant, Good technologies, Endgame. Anciennes participations : Fortify, ArcSight (deux entreprises rachetées par HP). Très récemment, le fond s'est attaqué au marché chinois en investissant dans des entreprises comme Venus tech. Son patron, Ted Schlein a été interviewé récemment dans Mag Secur[13].
Andreessen Horowitz	12	Morta Security, Lookout (blocage de malware et spyware sur appareils mobiles)
Draper Fisher Jurvetson	12	Good, Ping Identity
Mayfield Fund	11	Elemental Cyber Security, Centrify
Allegis Capital	10	Solera Networks (detection d'intrusion), Symplified, Ironport Systems, Bracket Computing, Shape.

[13]http://www.mag-securs.com/News/tabid/62/articleType/ArticleView/articleId/29689/Le-futur-de-la-securite-informatique-vu-par-un-investisseur-en-capital-risque.aspx

Shasta Ventures	9	Zenprise, Mocana, Fin Sphere,
August Capital	9	ThreatMetrix (Cybercrime Defender Platform), Splunk
Sigma Partners LLC	9	Oversight Systems

L'une des spécificités américaines en matière de *private equity* est la présence très forte sur le marché de l'IT et de la cybersécurité du fonds de la communauté américaine du renseignement, In Q Tel. Lancé en 1999, cette organisation à but non lucratif (tous les profits sont réinvestis dans le portefeuille) joue un rôle d'investisseur stratégique et prend des participations limitées, généralement comprises entre 500 000 et 2 millions de dollars, dans de jeunes start-up en phase d'amorçage ou de développement initial.

Le portefeuille d'In Q Tel couvre aujourd'hui aussi bien le renseignement que la sécurité, le « big data », l'énergie, le calcul intensif ou bien encore le cloud computing. Sur 55 entreprises en portefeuille à l'heure actuelle, 10 peuvent ainsi être considérées comme des « pure players » en cybersécurité : FireEye (dont l'introduction en bourse pourrait avoir lieu prochainement), Mocana, Oculislab, Veracode, Tyfone, Threatmetrix, Tenable Network Security, Silver Tail systems[14], Reversing Labs, Redseal networks. Parmi les anciennes participations du fonds : les sociétés ArcSight, Corestreet, Safeweb, Decru (chiffrement) ou Netapp.

L'efficacité du dispositif est telle que le gouvernement britannique envisageait fin 2011 de créer un In Q Tel britannique avec la participation du GCHQ.

[14]Société spécialisée dans l'analyse comportementale et la détection des fraudes sur le web. Elle a été positionnée par Gartner en « leader » dans son « quadrant magique » dédié à la détection de la fraude web.

1.4 Des marchés financiers enthousiastes

Les valeurs de la cybersécurité figurent au palmarès des recommandations des analystes financiers qui soulignent le niveau de la menace et l'importance de la commande publique. Ces valeurs sont la plupart du temps technologiques mais on y trouve aussi des sociétés de conseil et de services comme CACI ou Booz Allen Hamilton[15].

On compte ainsi de nombreuses introductions en bourse réussies ces dernières années :

- Splunk, spécialisé dans la sécurité des données, a vu ses actions bondir de 65 % après son introduction en avril 2012 ;
- Palo Alto Networks a grimpé de 26 % lors de son introduction en juillet 2012 ;
- Imperva (maison mère de Incapsula Inc.), spécialisée dans la sécurité des données, a vu ses actions progresser de 30 % le premier jour en novembre 2011.

1.5 Des grands groupes tres actifs

Plutôt que de développer leurs activités de cybersécurité par une croissance organique, nombre de grands groupes ont enfin opté pour le rachat d'entreprises spécialisées. En moyenne, selon une étude de PwC, les fusion-acquisition dans le domaine s'élèvent à environ 6 milliards de dollars par an depuis 2008[16]. Avec une très large majorité de deals aux Etats-Unis.

En dehors des investisseurs financiers, les entreprises qui achètent sont de trois types :

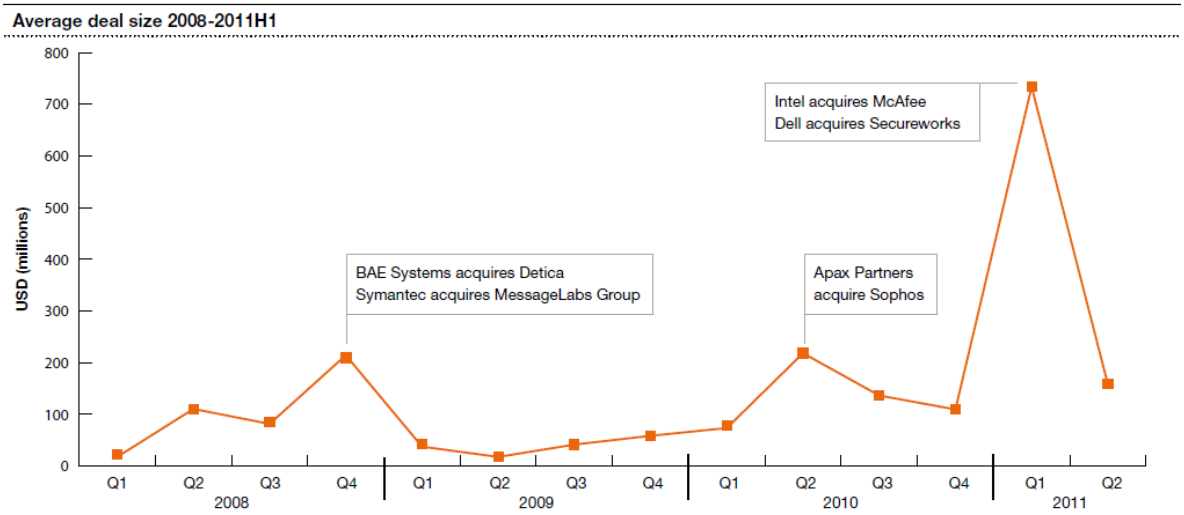
- Des éditeurs spécialisés en sécurité. Exemples : le rachat de Secure Computing par McAfee en 2008 ou celui de VeriSign par Symantec en 2010 pour 1,8 milliard ;
- Des sociétés IT (éditeurs logiciels, fabricants de hardware, intégrateurs…). Ces derniers interviennent généralement dans un second temps pour racheter des acteurs de taille déjà importantes ayant déjà procédé à des opérations de croissance externe auprès d'acteurs spécialisés. Exemples : le rachat de McAfee par Intel pour 7,8 milliards de dollars en février 2011, celui de SecureWorks par Dell pour 612 millions de dollars, celui de ArSight par HP en

[15] http://beta.fool.com/kprogers/2012/09/22/3-great-cyber-security-stock-plays/12387/
[16] http://www.pwc.fr//assets/files/pdf/2012/03/pwc_etude_cyber_security_m-and-a_2012-03-30.pdf

2010 pour 1,5 milliard de dollars, celui de VirusTotal par Google en 2012, d'Authentec par Apple en 2012 ;

- Des industriels de la défense. Ceux-ci voient dans la cybersécurité un moyen de capter des marchés gouvernementaux dans un secteur connexe et épargné par les coupes budgétaires. Exemples : Argon ST par Boeing en 2010, Applied Signal Technology par Raytheon en 2011, Norkom Group et Detica par BAE systems (Grande-Bretagne).

Evolution des acquisitions 2008-2011[17]



1.6 Quelles perspectives ?

Le dynamisme du secteur de la cybersécurité aux Etats-Unis est indéniablement basé sur un cercle vertueux reposant sur :

- Un vaste tissu de startups et PME très innovantes qui trouvent à chaque étape de leur développement des investisseurs appropriés ;

- Des grands groupes qui facilitent l'accès au marché aux plus petits, tant à l'export qu'au plan domestique. La filière s'est aussi organisée sous la bannière de l'organisation TechAmerica qui est issue de la fusion en 2004 de la Cyber Security Industry Alliance (CSIA), de l'American

[17] http://www.pwc.fr//assets/files/pdf/2012/03/pwc_etude_cyber_security_m-and-a_2012-03-30.pdf

Electronics Association (AeA), de l'Information Technology Association of America (ITAA) et de la Government Electronics & Information Technology Association (GEIA). TechAmerica remet chaque année un prix « Cyber Security & Authentication » lors des American Technology Awards ;

- Une offre de produits et services de plus en plus mature parce que davantage centrée sur les besoins utilisateurs ;

- Des marchés publics considérables, en particulier auprès de la NSA et du DHS, complétés par des marchés privés en progression ;

- Un volontarisme politique sans faille, basé notamment sur une collaboration public/privé toujours plus importante (cf. le dernier *executive order* présidentiel sur la protection des infrastructures critiques).

Le risque de bulle parait donc aujourd'hui limité et ne concerner que les marchés de défense fédéraux, pour lesquels les anticipations des grands groupes de la défense restent souvent trop élevées. « *Souvenez-vous de ce qui s'est passé avec les « dot commers »,* souligne le général Harry Raduege, ancien patron de la DISA et aujourd'hui directeur du Center for Cyber Innovation de Deloitte[18] *: un certain nombre se sont effondrés sur eux-mêmes ou ont échoué. Mais d'autre sont devenus des leaders du marché. Le cyber est un point focal et chacun veut en tirer parti. Certaines idées survivent, d'autres disparaissent. C'est un processus d'élimination naturel* ».

L'une des principales difficultés reste l'évaluation des marchés fédéraux : comment distinguer ce qui relève spécifiquement de la cybersécurité des besoins IT ou « cyber » génériques lorsque le Pentagone explique disposer de 66 000 personnes spécialisées en cybersécurité ? De fait, même si les besoins sont bien réels, ceux qui espèrent compenser la diminution des budgets des grands programmes de défense traditionnels par des projets « cyber » risquent d'être déçus. Les montants de ces derniers n'atteindront *a priori* jamais ceux de programmes conventionnels. Par ailleurs, la structure et la rentabilité des contrats de cybersécurité sont différentes : les contrats sont plus nombreux mais de taille plus modeste et surtout offre des rentabilités largement inférieurs à ceux des grands programmes d'équipement des décennies précédentes. Il revient donc aux industriels d'adapter leurs offres (notamment en intégrant des produits), leurs prix, mais aussi leurs coûts de structure, à cette nouvelle donne.

Lawrence Prior, executive vice-president de BAE déclarait en 2011[19] : « il y a eu beaucoup d'exagération sur ce marché. C'est un vrai marché. Il y a une croissance réelle. Mais c'est une croissance à un chiffre ou à deux chiffres en fonction du segment que vous ciblez. Pas à trois chiffres. » Quelques corrections sont ainsi à craindre du côté des grands industriels de la défense, à

[18] http://www.defensenews.com/article/20130304/DEFREG02/303040015
[19] http://www.ft.com/cms/s/0/1c406986-6b10-11e1-9781-00144feab49a.html#axzz2PD1SDcaO

l'image de General Dynamics, qui a annoncé en janvier une dépréciation d'actifs de 2 milliards de dollars en 2012 en raison de résultats moins bons que prévus dans le domaine IT, et notamment la cybersécurité. Mais il ne s'agit pas pour autant d'une bulle similaire à la bulle dot.com. « Tant que nous ne voyons pas des sociétés de cybersécurité racheter des sociétés de défense (un « SourceFire Lockheed » ?), nous sommes loin de la bulle dot.com », souligne la société Delling Advisory sur son blog[20]. Par ailleurs, si les sociétés de cybersécurité sont devenues une cible pour les industriels de la défense, elles ne représentent selon le Jane's Defence que 14 % des acquisitions des groupes de défense sur 2011.

[20] http://www.dellingadvisory.com/blog/2013/3/7/is-there-a-bubble-in-cyber-security-company-valuations

2. Stratégies cyber des Etats arabes du Golfe

Le Moyen-Orient apparait comme une zone particulièrement sensible aux cyber-risques. Le secteur de l'énergie (pétrole et gaz) est une cible privilégiée des pirates informatiques (Etats, groupes hacktivistes ou particuliers). Ce constat s'impose depuis la découverte de nombreuses cyberattaques (Flame[21], mais aussi Madi[22] et Gauss[23]) visant les infrastructures critiques, les institutions financières et les agences gouvernementales de pays du Moyen-Orient. Si ces menaces ont été découvertes en 2012, leur création daterait de bien plus longtemps. Découvert en mai 2012, Flame aurait été créé en 2006, selon l'éditeur en sécurité Symantec.

Aussi, les technologies de l'information et de la communication sont perçues comme un levier de développement endogène pour ces pays. Des sommes importantes y sont consacrées. Dans ce contexte, les entreprises occidentales y voient un marché juteux et n'hésitent pas à investir sur place en matière soit d'outils de protection (hardware et software), soit de services de conseil en cybersécurité (à l'image de la stratégie de lutte contre les APT proposée par Cassidian CyberSecurity et Netasq).

Les Etats arabes du Golfe semblent prendre conscience de l'importance de ces problématiques de cyberdéfense ; et ce, en dépit de niveaux de cybersécurité et de cyberdéfense (législation opérationnelle, stratégie de cyberdéfense, institutions dédiées, etc.) disparates. Le Cyber Defence Summit tenu à Muscat, Oman, les 4 et 5 mars témoigne de cette dynamique[24].

Les ministres de l'intérieur des pays membres du Conseil de coopération du Golfe se sont également rencontrés le 13 mars à Riyad. Ils ont consacré une grande part de cette rencontre aux techniques de surveillance des réseaux sociaux, sur Internet ou téléphones portables. Objectif : se doter d'une « cyberpolice ». Plus précisément, il s'agit de contrôler l'activisme des mouvements djihadistes et de divers mouvements d'opposition aux monarchies du Golfe en se dotant d'une force dédiée. Un projet de centre technique placé sous l'égide du CCG a été évoqué.

Cinq pays ont été analysés (Arabie Saoudite, Bahreïn, Oman, Qatar, Emirats Arabes Unis) sous le prisme des critères des fiches pays de l'Observatoire du Monde Cybernétique.

[21] http://www.symantec.com/connect/blogs/have-i-got-newsforyou-analysis-flamer-cc-servers

[22] http://me.kaspersky.com/en/about/news/virus/2012/Kaspersky_Lab_and_Seculert_Announce_Madi_a_Newly_Discovered_Cyber_Espionage_Campaign_in_the_Middle_East

[23] http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts

[24] http://www.cyberdefencesummit.com/

1.7 Arabie Saoudite

1.7.1 Infrastructures

Le **taux de pénétration Internet** sur le territoire de l'Arabie Saoudite calculé pour l'année 2012 est estimé à **43,6%**[25]. Le taux de pénétration de la **téléphonie mobile** s'élève à **14,52%**[26].

L'Arabie Saoudite possède **5** ***datacenters***[27] ; est équipée de **114** ***autonomous systems***[28] pour une population d'environ 28 000 000 d'habitants, ce qui représente une moyenne de un *datacenter* pour 245 600 habitants.

Alcatel-Lucent a signé un contrat de plusieurs millions d'euros en 2010 avec la Saudi Telecom Company (STC) pour l'extension du réseau d'accès haut débit de l'Arabie Saoudite. STC souhaitait proposer des applications de pointe et consommatrices de bande passante à ses clients, étendre la couverture de son réseau et bénéficier de capacités de transport et d'agrégation plus importantes.[29]

1.7.2 Capacités scientifiques et techniques

Des formations en informatique existent en Arabie Saoudite, toutefois les plaquettes officielles des universités ne précisent pas s'il s'agit de formations en « cyberdéfense ». Ainsi, la King Sauf University et la King Abdulaziz University possèdent chacune une division « *Computer and Information Sciences* ».[30] [31]

1.7.3 Base industrielle et technologique

Si l'économie du pays est centrée sur l'exploitation pétrolière, les autorités saoudiennes souhaitent anticiper l'après-pétrole et misent sur les technologies de l'information et de la communication pour soutenir la croissance. L'exemple le plus frappant reste la « Cité des technologies de l'information et des communications » financée grâce à un partenariat public-privé à hauteur de 100 milliards de dollars[32].

[25] http://www.internetworldstats.com/list2.htm
[26] http://www.indexmundi.com/g/r.aspx?v=4000&l=fr
[27] http://www.datacentermap.com/
[28] http://www-public.it-sudparis.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html
[29] http://www.sicavonline.fr/index.cfm?action=m_actu&ida=471643-alcatel-lucent-contrat-de-plusieurs-millions-d-euros-en-arabie-saoudite
[30] http://ksu.edu.sa/colleges/ScienceColleges/Pages/default.aspx
[31] http://computing.kau.edu.sa/Default.aspx?Site_ID=611&Lng=EN
[32] http://www.lefigaro.fr/economie/2007/06/25/04001-20070625ARTFIG90262-l_arabie_saoudite_reve_de_villes_nouvelles.php

Fait plus surprenant, le prince saoudien Al-Walid a investi, en 2011, 300 millions de dollars dans la société de microblogging Twitter, avançant que « les médias sociaux vont fondamentalement changer le paysage de l'industrie des médias dans les prochaines années »[33].

Le marché des services informatiques de l'Arabie Saoudite est le plus important de tous les pays arabes[34], avec un chiffre d'affaire d'environ 1,2 milliards de dollars en 2012[35].

Le marché de l'industrie logicielle représente en 2012 772 millions de dollars[36].

L'Organisation Saoudienne de Normalisation, Métrologie et Qualité (SASO) est membre de la Commission électronique internationale (CEI).[37]

1.7.4 Sécurité et gouvernance des réseaux

1.7.4.1 Ecosystème cybercriminel et hacktiviste

Comme de nombreuses Nations ayant développé leur connectivité, l'Arabie Saoudite fait l'objet de nombreuses attaques informatiques de la part de groupes de hackers. Selon un rapport rendu public par Symantec, en 2012, la cybercriminalité a coûté 2,6Md€ à l'Arabie Saoudite.[38] Il est estimé que pendant cette même période, 3,6 millions de personnes auraient été victimes de la cybercriminalité, subissant en moyenne une perte financière de 195 dollars. De plus, 40% des utilisateurs de réseau sociaux ont été victimes de cybercriminalité à partir de ces plates-formes.

En 2012, l'entreprise pétrolière Saudi Aramco a fait l'objet d'une cyberattaque. L'attaque aurait été réalisée grâce à l'implication d'acteurs internes à l'entreprise et aurait touché 30 000 ordinateurs effaçant les contenus de leurs disques durs, et permettant le vol de données jugées sensibles[39]. Le groupe de *hackers* dénommé « *Cutting Sword of Justice* » a revendiqué la cyberattaque, dénonçant le soutien du régime saoudien aux actes commis par des pays voisins dans la région. Ainsi cette cyberattaque est censée être un « avertissement » aux tyrans[40].

Bien que le même groupe ait menacé une deuxième fois l'entreprise saoudienne le 25 août 2012, peu de temps après la première attaque, certains analystes ont formulé une autre hypothèse : la

[33] http://www.leparisien.fr/flash-actualite-economie/arabie-le-prince-al-walid-investit-300-millions-de-dollars-dans-twitter-19-12-2011-1775330.php
[34] http://www.rncos.com/Press_Releases/Saudi-Arabias-IT-Industry-All-Set-to-Grow-at-a-Fast-Pace.htm
[35] http://www.marketresearch.com/Business-Monitor-International-v304/Saudi-Arabia-Information-Technology-Q3-7094930/
[36] http://www.marketresearch.com/Business-Monitor-International-v304/Saudi-Arabia-Information-Technology-Q3-7094930/
[37] http://www.iec.ch/dyn/www/f?p=103:5:0##ref=menu
[38] http://www.arabnews.com/saudi-arabia/cybercrime-costs-saudi-arabia-sr-26-bn-year
[39] http://econflicts.blogspot.fr/2012/09/news-cyber-attaque-contre-saudi-aramco.html
[40] http://pastebin.com/HqAgaQRj

cyberattaque aurait été perpétrée par l'Iran afin de décourager la société Saudi Armaco d'augmenter sa production pétrolière en vue de compenser la diminution des livraisons opérées par l'Iran[41].

En termes d'hacktivisme, l'affaire la plus médiatique concerne ce pirate saoudien, « *OxOmar* », membre du groupe « groupe-xp », et qui avait revendiqué en janvier 2012 plusieurs attaques prenant pour cible des sites israéliens[42]. Baptisé par les média israéliens le « hacker saoudien », ce dernier avait quelques mois plus tard succombé à une crise d'asthme, tandis qu'il venait d'être nommé à un poste dans la fonction publique[43]. Ce dernier avait attaqué plusieurs sites dont ceux de ministères israéliens, la bourse de Tel Aviv et le site de la compagnie israélienne El Al, avant de divulguer les coordonnées de plus de 20 000 cartes de crédit. Le groupe de hackers avait proclamé, à l'époque, être en mesure de publier les coordonnées de plus de 400 000 cartes de crédit.

1.7.4.2 Cadre juridique de la lutte contre la cybercriminalité

L'Arabie Saoudite dispose d'une loi relative à la cybercriminalité, soumise par le Conseil des Ministres par la décision n° 79, en date du 7/3/1428 (26 mars 2007)[44], et approuvée par Décret royal.

Le texte de loi est composé de 16 articles, qui dressent le cadre général de la cybercriminalité dans le pays. Ainsi le texte définit les termes appropriés à ce champ d'activités (article 1), avant d'évoquer les objectifs de cette loi (article 2) et de lister les actes passibles de sanctions (article 3). Les peines de prison maximales sont de 10 ans d'emprisonnement et une amende de 5 millions de riyal (article 5)[45].

Table I: Anti Crime Act 2007

No.	Type of Crime	Penalty
1	Hacking, Net Extortion, Website Defacement	SR 5,00,00 or 1 Year or both
2	Spoofing, Credit Card Fraud	SR 20,00,000 or 3Years or both
3	Denial of Service, Software Piracy, Data Diddling	SR 30,00,000 or 4Years or both
4	Virus Dissemination, Pornography, Illegal Trade	SR 30,00,000 or 5 Years or both
5	Cyber Terrorism	SR 50,00,000 or 10 Years or both

[41] http://www.pcworld.com/article/261320/kill_timer_found_in_shamoon_malware_suggests_possible_connection_to_saudi_aramco_attack.html

[42] http://leclicenmoins.wordpress.com/2012/01/13/des-hacktivistes-de-plus-en-plus-actifs-au-moyen-orient/

[43] http://www.terredisrael.com/infos/le-hacker-saoudien-est-mort-dune-crise-dasthme/

[44] http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Pages/CybercrimesAct.aspx

[45] http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf

Ainsi différents types de cybercrimes peuvent être commis et sont répertoriés comme tels en Arabie Saoudite. Il en existe huit différentes formes : *hacking*, *pornographie*, *attaque par déni de service*, *dissémination de virus*, *piratage de logiciels*, *defacement de sites web*, *cyberterrorisme*, *échanges illégaux sur Internet* et *phishing*.[46]

Le cadre de la lutte contre la cybercriminalité dépasse parfois l'aspect juridique. Les autorités saoudiennes utilisent néanmoins cette notion afin de censurer un grand nombre de sites Internet et de mener un filtrage très strict. Les autorités auraient ainsi bloqué environ 400 000 sites qui ne répondent pas à leurs critères d'admissibilité[47]. Les sites politiques comme Elaph, ou encore les sites dits participatifs, sont tout particulièrement visés par les autorités chargées de cette régulation.

De même, les autorités du pays ont mis en place une surveillance accrue des utilisateurs Internet. D'une part dans les cybercafés, ces derniers devant fournir une liste des clients et des sites consultés, refuser l'accès pour les mineurs et fermer tout accès après minuit. D'autre part, depuis l'acceptation de BlackBerry de donner accès, sur mandat judiciaire, à certains messages privés[48].

Depuis 2011, les autorités saoudiennes ont entériné de nouvelles dispositions législatives tout aussi restrictives et limitant une utilisation libre et totale d'Internet. Ces mesures visent à renforcer la censure, mieux contrôler les médias et empêcher autant que faire se peut le développement de blogs liés à l'opposition politique ou à des dissidents. Les quelques blogueurs qui ont évoqué ce sujet se sont pour la plupart retrouvés arrêtés. L'une des possibilités, offerte par le nouveau règlement, permet désormais au ministère de l'Information et de la Culture de choisir le rédacteur en chef de tous les journaux électroniques[49].

Dans l'objectif de mieux réagir à toute attaque informatique, l'Arabie Saoudite est équipée d'un CERT[50]. De plus, le pays dispose d'un « *Internet Services Unit* » qui est chargé de veiller au bon filtrage des pages Internet afin de bloquer celles qui sont ciblées par les autorités[51].

1.7.5 Capacité de lutte informatique

La position de l'Arabie Saoudite est particulière d'un point de vue géopolitique : alliée des Etats-Unis avec qui elle cherche à développer des programmes de défense, elle occupe dans la région une place dominante en matière de cybersécurité.

---

[46] https://docs.google.com/viewer?a=v&q=cache:AzK1vkFvBhcJ:ijarcet.org/index.php/ijarcet/article/view/468/PDF+&hl=fr&gl=fr&pid=bl&srcid=ADGEEShlkRPYFoRSK1WCcw-lUzQH77WTyMhiKuSG-8eYeUpC4-MUWrX4jyXRTgt5lPo8QgfErDrltyi3gObqefHRFZfJ3NBE1vDngslzWIeGj_gPbbsBTLH9SqQIG1MD5J7Df8XMgnP9&sig=AHIEtbRGFP29khxHVxfAGdUU5D00xjHdZw

[47] http://fr.rsf.org/internet-enemie-arabie-saoudite,39703.html

[48] Ibid.

[49] http://fr.rsf.org/arabie-saoudite-nouvelles-regulations-liberticides-08-01-2011,39244.html

[50] http://cert.gov.sa/index.php?option=com_frontpage&Itemid=1

[51] http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm

L'actualité des gouvernements occidentaux, touchés par de multiples cyberattaques, a conduit les autorités saoudiennes à étudier et analyser les cyberstratégies mises en œuvre par ces derniers, afin de disposer d'un cadre doctrinal satisfaisant. Ainsi le Général Naef Bin Ahmed Al-Saud a proposé un « *Saudi Outlook for Cybersecurity Strategies Extrapolated From Western Experience* » et a pu rendre compte des principales problématiques concernant la cybersécurité[52].

Le principal élément qui ressort de cette analyse est la nécessité, pour les autorités saoudiennes compétentes, de prendre la mesure des besoins « cyber » du pays, non seulement au niveau théorique, mais également à un niveau pragmatique. Autrement dit, combien d'emplois, pour quelles compétences, face à quelles menaces ?

Pour lutter contre ces dernières, l'Arabie Saoudite envisage de dépenser 33 milliards de dollars d'ici 2018 en matière de cybersécurité[53].

De plus, suite à la cyberattaque menée à l'encontre du groupe pétrolier Aramco, les autorités saoudiennes ont décidé de mettre en place une unité de cybersécurité, après avoir embauché des consultants américains afin de réaliser un diagnostic des exigences de protection pour le réseau informatique du pays[54].

1.8 Bahreïn

1.8.1 Infrastructures

Le **taux de pénétration Internet** sur le territoire du Bahreïn calculé pour l'année 2012 est estimé à **57,1%**[55]. Le taux de pénétration de la **téléphonie mobile** s'élève à **22,76%**[56]**.**

Le pays possède **4** ***datacenters***[57] ; il est équipé de **27** ***autonomous systems***[58] pour une population supérieure à 1 325 000 habitants, ce qui représente une moyenne de un *datacenter* pour environ 49 000 habitants.

En novembre 2012, l'extension (.br) arrive en 12ème position derrière le (.eu).

[52] http://www.ndu.edu/press/lib/pdf/jfq-64/JFQ-64_75-81_Al-Saud.pdf
[53] http://blog.inkerman.com/index.php/2012/04/04/not-if-but-when-businesses-and-cyber-security/
[54] http://www.independent.co.uk/news/world/americas/cyberwar-poses-dilemma-for-us-defence-exporters-8346311.html
[55] http://www.internetworldstats.com/list2.htm
[56] http://www.nationmaster.com/graph/med_mob_pho-media-mobile-phones
[57] http://www.datacentermap.com/
[58] http://www-public.it-sudparis.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html

1.8.2 Capacités scientifiques et techniques

Des formations en informatique existent au Bahreïn, toutefois les plaquettes officielles des universités ne précisent pas s'il s'agit de formations en « cyberdéfense ». Ainsi, la Applied Science University, la Delmon University for Science and Technology ou encore la Ama International University possèdent chacune une division « *Computer and Information Sciences* ».[59]

Le Centre régional pour les technologies de l'information et de la communication situé à Manama souhaite quant à lui favoriser l'implantation et l'utilisation des TIC dans l'acquisition et le partage des connaissances[60].

1.8.3 Base industrielle et technologique

Le marché des TIC au Bahreïn était évalué à 375 billions de dollars en 2010, en raison d'une demande croissante des entreprises en la matière. Le pays mise sur l'e-commerce et l'e-gouvernement. Leur objectif étant de disposer de 90% des services administratifs en ligne[61].

De nombreux acteurs des TIC à l'échelle internationale disposent de bureaux au Bahreïn : WIPRO, Netgear, Cisco, Tata Consultancy Services, Huawei…

1.8.4 Sécurité et gouvernance des réseaux

1.8.4.1 Ecosystème cybercriminel et hacktiviste

Selon l'activiste bahreïni Nabil Rajab, le Bahreïn est « le pays le plus actif sur Twitter dans le monde arabe » et offre ainsi un autre visage de l'hacktivisme[62].

L'Organisation *Bahrain Watch* prétend que les autorités du Bahreïn espionnent les activistes de l'opposition à l'aide d'un logiciel malveillant qui proviendrait, selon des sources de cette organisation, d'une entreprise britannique[63].

C'est ce que prétendent Bill Marczak, membre fondateur de l'Organisation *Bahrain Watch*, et Morgan Maquis-Boire, chercheur au *Citizen Lab*, qui ont analysé une série de mails suspicieux envoyés à des activistes en juin et juillet 2012[64]. Le logiciel malveillant serait *FinFisher*, vendu par la

[59] http://www.4icu.org/bh/
[60] http://www.unesco.org/new/fr/communication-and-information/about-us/how-we-work/category-2-institutes-and-centres/bahrain/
[61] http://www.bahrainedb.com/uploadedFiles/Bahraincom/OpportunitiesInBahrain/Informaton%20Technology,%202009.pdf
[62] http://owni.fr/2012/05/08/assange-interroge-les-revoltes-arabes/
[63] http://www.free-press-release.com/news-bahrain-watch-identifies-spying-activity-by-the-government-of-bahrain-1343267696.html
[64] https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/3/

société britannique Gamma Group[65]. L'activiste Nabil Rajab a notamment souligné que « des activistes sur Twitter ont été emprisonnés, certains torturés à mort ».

Les Anonymous se sont eux aussi emparés de la révolution en piratant, courant 2012, des sites internet de chaines de télévision et en procédant à des attaques DDoS[66] dans le cadre de l'opération « #OpBahrain ».

En mars 2012, Reporter Sans frontières classait le Bahreïn comme « Ennemi d'Internet »[67].

Enfin, une étude dénombrait qu'en 2012, 16% des ordinateurs au Bahreïn étaient infectés[68].

1.8.4.2 Cadre juridique de la lutte contre la cybercriminalité

Très peu d'informations traitent du cadre juridique de la lutte contre la cybercriminalité.

Le Bahreïn est équipé d'un CERT, créé en novembre 2012[69]. De plus, le pays dispose d'une cyberpolice depuis 2004, qui aurait constaté une forte progression de la cybercriminalité depuis 2006 : en effet la cybercriminalité aurait été multipliée par 10 depuis cette date[70].

Fin 2012, des discussions étaient prévues au Parlement afin de mettre en place une réglementation plus stricte en matière de cybercriminalité. Des sanctions pécuniaires et des périodes d'emprisonnement étaient alors envisagés.

1.8.5 Capacité de lutte informatique

La préoccupation des autorités du Bahreïn en matière de cyberdéfense n'est pas récente et recouvre une vision à long terme. En témoigne la stratégie VISION 2030 mise en œuvre à l'intérieur du pays, ou encore la conférence sur la Sécurité en ligne, qui s'est tenue en avril 2010, sous l'égide de l'Autorité de Régulation des Télécommunications (TRA). Il s'agissait alors de la première conférence de ce type dans la région[71].

Si la première concerne de façon plus générale l'économie du pays, il s'agissait pour les auteurs de cette étude de démontrer l'utilisation possible et innovante d'Internet comme un instrument au service d'un objectif de croissance économique et de bien-être[72].

---

[65] http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html
[66] http://www.undernews.fr/hacking-hacktivisme/opbahrain-anonymous-pirate-le-site-f1-racers.html
[67] http://12mars.rsf.org/i/Rapport_Ennemis_Internet_2012.pdf
[68] http://www.gulf-daily-news.com/Print.aspx?storyid=254367
[69] http://www.ameinfo.com/bahrains-reload-consulting-launches-computer-emergency-317567
[70] http://hackread.com/new-crackdown-on-cyber-crime-in-bahrain/
[71] http://www.fosigrid.org/middle-east/bahrain
[72] http://www.tra.org.bh/en/pdf/Vision2030Englishlowresolution.pdf

En octobre 2010, la TRA a ainsi pu rendre public son rapport « *State of The Nation Review of Internet Safety 2010* », qui analysait et identifiait les problématiques liées à la sécurité en ligne et les failles rencontrées à l'époque par les différents utilisateurs, publics ou privés. Le rapport proposait quelques recommandations, notamment liées au renforcement du cadre juridique, qui apparaît insuffisant[73]. De même, le rapport évoquait la nécessité d'entraîner les officiers de la cyberpolice afin qu'ils soient préparés de la meilleure façon possible à la cybercriminalité.

C'est d'ailleurs du fait de cette volonté d'entraînement et de formation des unités de cyber police que Bahreïn a développé un partenariat avec Interpol. Ainsi, une formation est envisagée en lien avec le « Complex for Innovation » de l'Organisation, censé ouvrir en 2014 à Singapour[74].

1.9 EMIRATS ARABES UNIS

1.9.1 Infrastructures

Le **taux de pénétration d'internet aux Emirats Arabes Unis était de 70,9%** en 2012[75], nettement inférieur à celui de la téléphonie mobile qui était de 149% en 2011[76].

Les Emirats Arabes Unis disposent d'**un point d'échange internet**[77], de **4 *datacenters*** basés à Mohammed Bin Zayed City et à Dubaï[78] et de 2 répliques anycast du serveur DNS racine de type F et K basés respectivement à Dubaï et Abu Dhabi[79]. 48 *Autonomous Systems* existent aux Emirats Arabes Unis, pour une population qui s'élève à 7 890 924 habitants[80]. Le pays est relié à l'internet par deux points de connexion[81].

4 opérateurs se partagent le marché de l'accès à internet aux Emirats Arabes Unis : Du, Etisalat, Precedence et OGER Telecom.

1.9.2 Capacités scientifiques et techniques

Quantité d'université des Emirats Arabes Unis proposent des formations en informatique de tous niveaux (bachelor, master ou autres diplômes)[82]. Ces formations concernent divers aspects des

[73] http://www.itp.net/583730-bahrain-reveals-first-ict-safety-review#.UUCxwjdnByV
[74] https://secure.interpol.int/Public/ICPO/PressReleases/PR2013/PR015.asp
[75] http://www.internetworldstats.com/me/ae.htm
[76] https://www.cia.gov/library/publications/the-world-factbook/geos/ae.html
[77] https://prefix.pch.net/applications/ixpdir/summary/
[78] http://www.datacentermap.com/
[79] http://www.root-servers.org/
[80] http://www-public.int-evry.fr/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html
[81] http://cyber.law.harvard.edu/netmaps/geo_map_home.php
[82] http://gulfnews.com/news/gulf/uae/education/gearing-up-for-cyber-warfare-1.798141

technologies de l'information, aussi bien le développement technologique que l'approche stratégique et théorique du sujet[83].

Le pays a récemment mis en place le « Fonds pour les TIC ». Première initiative de ce type au Moyen-Orient, le fond a pour finalité de proposer des bourses aux personnes souhaitant travailler dans le secteur des TIC et d'apporter une aide à la création d'établissements dispensant un enseignement dans ce domaine[84].

1.9.3 Base industrielle et technologique

Le marché des télécommunications des Emirats arabes unis est passé de 8,2 milliards USD en 2005 à 13,6 milliards en 2011, soit un taux de croissance annuel de 20%.

Le « Fonds pour les TIC » a également pour finalité de soutenir les projets de recherche-développement novateurs. Il accordera une aide aux entreprises startups, proposera des incubateurs et apportera une aide à la création d'institutions de recherche-développement[85].

1.9.4 Sécurité et gouvernance des réseaux

1.9.4.1 Ecosystème cybercriminel et hacktiviste

En 2012, un raid mené par les autorités a abouti à la fermeture de nombreuses organisations civiles ou d'oppositions ainsi qu'à l'arrestation de plusieurs hacktivistes, incluant le blogger Ahmed Adb al-Khaleq[86].

Citizen Lab a publié un rapport dans lequel il identifie un possible lien entre la compagnie de logiciels italienne, Hacking Team, et un virus qui a infecté l'ordinateur d'un dissident des Emirats Arabes Unis favorable à la démocratie en 2012.

Concernant l'ensemble de la population, et non uniquement l'écosystème cybercriminel ou hacktiviste, plus de 50 000 ordinateurs aux Emirats Arabes Unis seraient infectés par des logiciels malveillants. C'est ce que révèle une étude réalisée par Trend Micro[87].

1.9.4.2 Cadre juridique de la lutte contre la cybercriminalité

Il n'existe pas aux Emirats Arabes Unis de loi spécifique relative à la protection des données, en revanche il existe certaines restrictions et amendes concernant le non-respect du caractère privé des

[83] http://www.hct.ac.ae/programs/computer-information-science/
[84] https://itunews.itu.int/Fr/2373-Linnovation-en-tete-du-programme-daction.note.aspx
[85] https://itunews.itu.int/Fr/2373-Linnovation-en-tete-du-programme-daction.note.aspx
[86] http://www.freedomhouse.org/article/revisions-uae-cybercrime-law-stifle-free-expression
[87] http://www.arabianbusiness.com/at-least-50-000-uae-computers-infected--41500.html#.UUC9OTdnByU

données. En effet la Constitution du pays de 1971 et le Code pénal de 1987 reprennent certaines définitions que l'on peut relier à la cybercriminalité[88].

De façon plus générale, les Emirats Arabes Unis dispose d'une loi relative à la cybercriminalité qui date de 2006. Celle-ci a été revue et corrigée en 2012, restreignant de façon stricte la liberté d'usage d'Internet et provoquant de vives réactions critiques de la part de nombreuses ONG. Si le texte prévoit la lutte contre le terrorisme, la pornographie et « l'insulte de la religion », il envisage également des peines d'emprisonnement pour « conspiration ou encore « appel à manifester »[89]. En mars 2012, les autorités avaient fermé les offices de nombreuses organisations civiles, dont l'Institut National pour la Démocratie (NDI)[90].

Le pays a signé un accord de coopération avec les Etats-Unis en matière de cybersécurité[91].

Les Emirats Arabes Unis disposent d'un CERT[92].

1.9.5 Capacité de lutte informatique

Les Emirats Arabes Unis cherchent, au même titre que les autres pays du golfe, à développer leurs capacités cyber. Pour ce faire, les Emirats Arabes Unis font appel à des entreprises étrangères pour fournir leur conseil sur le développement d'outils et de cadres stratégiques de cyberdéfense. La société américaine CyberPoint aurait ainsi été sollicitée par les Emirats Arabes Unis[93].

En septembre 2012, le pays a instauré l'Autorité Nationale de Sécurité Electronique pour se protéger des cybermenaces, dans une démarche officiellement purement défensive[94].

Les Emirats Arabes Unis ont accueilli en mars 2012 la conférence sur la Sécurité Internationale et la Résilience Nationale, durant laquelle une journée entière a été consacrée à la cybersécurité. Cet événement s'inscrit dans la volonté nationale et régionale de développer une stratégie de cybersécurité et de cyberdéfense, jusqu'à présent officiellement défensive, la priorité des autorités étant d'assurer la protection des réseaux informatiques du pays[95].

[88] http://www.ameinfo.com/cybercrime-uae-313655
[89] http://www.courrierinternational.com/breve/2012/11/13/une-nouvelle-loi-repressive-contre-la-cyber-dissidence
[90] http://www.freedomhouse.org/article/revisions-uae-cybercrime-law-stifle-free-expression
[91] http://usuaebusiness.org/2013/03/u-s-u-a-e-business-council-partners-promote-u-s-u-a-e-industry-and-trade-partnership-in-northern-california/
[92] http://www.aecert.ae/about-us.php
[93] http://www.independent.co.uk/news/world/americas/cyberwar-poses-dilemma-for-us-defence-exporters-8346311.html
[94] http://www.independent.co.uk/news/world/americas/cyberwar-poses-dilemma-for-us-defence-exporters-8346311.html
[95] http://www.commsmea.com/11996-uae-tra-tackles-threat-of-cyber-war/#.UUC9tdZnSuI

1.10 OMAN

1.10.1 Infrastructures

Le **taux de pénétration Internet** en Oman était de **68%** au 30 juin 2012[96]. Le taux de pénétration de la téléphonie mobile lui était nettement supérieur, s'élevant à 169% en 2011[97].

Le sultanat d'Oman ne dispose d'**aucun point d'échange Internet**[98], mais bénéficie d'un *datacenter* basé à Muscat[99], ainsi que de **5 *autonomous systems***, pour une population de 3 090 150 habitants en 2012[100]. Le pays est connecté au reste du monde par un unique point de connexion[101] et n'a aucun serveur racine DNS[102].

Deux fournisseurs d'accès à Internet existent en Oman (Oman Tel Networks et Nawras), mais un seul (Omantel) fournissait de l'ADSL en 2012[103].

Le marché de l'internet mobile est lui partagé entre six fournisseurs, dont deux principaux leaders : Apna Mobile (partenaire de Nawras) et Friendi[104].

1.10.2 Capacités scientifiques et techniques

La quasi-totalité des universités du pays proposent des formations en informatique. Essentiellement axées sur l'ingénierie informatique, ces formations de type *bachelor* ou *master* concernent également l'aspect business des technologies de l'information. Le sultanat d'Oman développe ainsi une large base technologique, profitable aussi bien à la recherche nationale qu'aux entreprises présentes dans le pays.

1.10.3 Base industrielle et technologique

Parmi les entreprises présentes dans le pays figurent notamment Cassidian CyberSecurity et Netasq, partenaires du Sommet de Cyberdéfense d'Oman, qui ont profité de cette occasion pour annoncer leur nouvelle stratégie de lutte contre les APT au Moyen-Orient[105].

---

[96] http://www.internetworldstats.com/middle.htm#om
[97] https://www.cia.gov/library/publications/the-world-factbook/geos/mu.html
[98] https://prefix.pch.net/applications/ixpdir/summary/
[99] http://www.bahwancybertek.com/data_center.html
[100] http://www-public.int-evry.fr/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html
[101] http://cyber.law.harvard.edu/netmaps/geo_map_home.php?cc=OM
[102] http://www.root-servers.org/
[103] http://www.muscatmutterings.com/2012/05/internet-in-oman.html
[104] http://www.prepaidmvno.com/mvno-companies/middle-east-mvno-companies/oman-mvno-companies/
[105] http://www.cassidian.com/ko/web/guest/press/-/asset_publisher/YMx3/content/id/161396

En mai 2012, Cassidian CyberSecurity a présenté, à l'occasion du forum « International Cyber Security Forum for Energy and Utilities », une solution de protection des systèmes de contrôle industriel de l'industrie pétrolière et gazière incluant un centre opérationnel de sécurité (SOC).[106]

1.10.4 Sécurité et gouvernance des réseaux

1.10.4.1 Ecosystème cybercriminel et hacktiviste

Une partie des condamnations pour cybercrimes concerne des faits relevant davantage de la liberté d'expression. Plus que des hacktivistes, il s'agirait davantage de bloggeurs dissidents appelant à des réformes démocratiques et condamnés pour des crimes de lèse-majesté[107].

La cybercriminalité existe cependant bien en Oman, puisqu'avec l'accroissement du nombre d'internautes, le piratage des comptes Facebook et Twitter s'est développé dans le pays[108]. Le développement de la cybercriminalité dans la région a même poussé Kaspersky à classer en 2011 le sultanat d'Oman dans un groupe de pays particulièrement vulnérables aux attaques : 41 à 60% des internautes de ces pays seraient exposés aux cybermenaces[109].

1.10.4.2 Cadre juridique de la lutte contre la cybercriminalité

Le sultanat d'Oman a adopté une loi sur la cybercriminalité en mai 2011[110]. Cette loi, plutôt que de définir la cybercriminalité, englobe quantité de méfaits perpétrés à l'aide de systèmes informatiques (dont le piratage, l'utilisation de logiciels malveillants, le phishing, la fraude, l'usurpation d'identité et notamment la délinquance en col blanc).

Ce cadre juridique souffre cependant d'un manque de connaissance des juges sur la question. En juin 2013 les participants d'un forum sur la cybercriminalité ont ainsi appelé à une meilleure formation des juges et des agents de la Police Royale, afin d'optimiser aussi bien la prévention et la détection des cybercrimes que le jugement des affaires cybercriminelles[111].

Reporters Sans Frontières a dénoncé en septembre 2012 la sévérité des sanctions définies à l'encontre de journalistes accusés de lèse-majesté et de cybercrimes. En plus d'amendes fiduciaires, des peines de prison ont été prononcées, pour des propos relevant selon Reporters Sans Frontières de la liberté d'expression[112].

---

[106] http://www.eads.com/eads/int/en/news/press.fr_20130305_cassidian_netasq_middle_east.html
[107] http://fr.alkarama.org/index.php?option=com_content&view=article&id=1245:oman-neuf-cyber-activistes-en-prison-pour-avoir-appele-a-des-reformes&catid=32:communiqu&Itemid=109
[108] http://oneoman.com/2012/04/04/oman-facebook-twitter-users-accounts-hacked/
[109] http://www.kaspersky.com/about/news/virus/2011/IT_Threat_Evolution_Q2_2011
[110] http://omanlawblog.curtis.com/2011/04/oman-cybercrime-law.html
[111] http://gulfnews.com/news/gulf/oman/oman-forum-calls-for-tough-laws-against-cybercrime-1.1035332
[112] http://en.rsf.org/oman-more-jail-sentences-on-cyber-crime-18-09-2012,43403.html

1.10.5 Capacité de lutte informatique

Peu d'informations sont disponibles sur les capacités de cyberdéfense d'Oman, mais il est certain qu'une forte volonté existe de la part des dirigeants omanis de développer les capacités cyber du pays et d'en faire la **plateforme de la cybersécurité du monde arabe**[113].

S'il est encore tôt pour parler de doctrine, il ne fait cependant aucun doute qu'une réflexion est menée sur la cyberdéfense en Oman, comme en témoigne l'organisation à Muscat du Sommet de cyberdéfense, dont 2013 fut la troisième édition[114].

Le Sultanat d'Oman souhaite devenir un acteur majeur de la lutte informatique au Moyen-Orient, et s'appuie pour cela sur des réflexions et échanges avec de nombreux partenaires étrangers, aussi bien publics que privés[115].

La désignation du CERT d'Oman comme centre régional de la cybersécurité par l'*International Telecommunications Union* (ITU) et l'*International Multilateral Partnership Against Cyber Threat* (IMPACT) va dans ce sens[116]. Avec une population de 235 millions d'habitants et une part croissante de 30% d'utilisateurs internet dans les pays arabes[117], les enjeux sont grands et les besoins existent, d'où le positionnement régional du Sultanat d'Oman, qui dépasse donc les prérogatives uniquement nationales et appelle à une collaboration entre Etats du monde arabe.

1.11 QATAR

1.11.1 Infrastructures

Le **taux de pénétration internet du Qatar était de 86,2%** en 2012[118], un pourcentage conséquent mais néanmoins nettement inférieur au taux de pénétration mobile qui était de 123% en 2011[119].

Aucun point d'échange Internet n'est enregistré au Qatar[120], mais le pays dispose de **3 *datacenters***, tous basés à Doha (M-VAULT 1, 2 et 3)[121]. **5 *autonomous systems*** existent dans le pays[122], pour une population de 1 951 591 habitants[123]. Deux points de connexion relient le Qatar à l'internet

[113] http://www.muscatdaily.com/Archive/Business/Muscat-to-host-Cyber-Defence-Summit-1x4i
[114] http://www.cyberdefencesummit.com/
[115] http://www.cyberdefencesummit.com/speakers/
[116] http://www.ameinfo.com/omans-cert-designated-regional-cyber-security-322828
[117] http://www.timesofoman.com/News/Article-9998.aspx
[118] http://www.internetworldstats.com/me/qa.htm
[119] http://www.internetworldstats.com/me/qa.htm
[120] https://prefix.pch.net/applications/ixpdir/summary/
[121] http://www.datacentermap.com/qatar/doha/
[122] http://www-public.int-evry.fr/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html
[123] https://www.cia.gov/library/publications/the-world-factbook/geos/qa.html

mondial[124], et deux répliques anycast du serveur DNS racine de type I et K sont enregistrées à Doha[125].

Deux fournisseurs d'accès à internet se partagent le marché : Ooredoo (anciennement Qatar Telecom mais rebaptisé en février 2013[126]) et Vodafone Qatar[127]. Qatar Telecom était en situation de monopole jusqu'en 2006 et la décision de l'instance suprême qatarie des communications et des technologies de l'information (ictQatar) de briser ce monopole.

Qatar Telecom ayant été en situation de monopole entre 1998 et 2006, la quasi-totalité des infrastructures de télécommunications reste sous son contrôle, Vodafone Qatar ne faisant qu'exploiter ces infrastructures pour formuler son offre.

Tous les deux proposent également des solutions internet mobiles, mais seul Ooredoo propose de la fibre optique et de la 4G[128].

En date du 13 mars 2013, **15 520 domaines Internet** ont été enregistrés par le registre des domaines du Qatar[129].

1.11.2 Capacités scientifiques et techniques

Au Qatar, trois universités proposent des formations en informatique : la *Qatar University* qui propose un master en sciences de l'informatique[130], la *Qatar Foundation* qui offre un programme d'informatique[131] et le *College of North Atlantic Qatar* qui lui dispose d'un département des technologies de l'information et propose donc divers diplômes autour des systèmes d'information concernant aussi bien le matériel que les logiciels[132]. Le développement d'une chaire de cybersécurité à l'université Carnegie Mellon est également envisagé[133].

Des centres d'apprentissage informatique proposent à Doha des cours d'*ethical hacking*, au cours desquels sont abordées des techniques de hacking mais également des réflexions autour de l'*ethical hacking*, de la sécurité des systèmes d'information et des lois internationales en la matière[134].

---

[124] http://cyber.law.harvard.edu/netmaps/mlic_20110513.pdf
[125] http://www.root-servers.org/
[126] http://www.gulf-times.com/qatar/178/details/343575/qtel-rebrands-as-ooredoo-in-major-global-initiative
[127] http://www.vodafone.qa/en/internet
[128] http://www.ooredoo.qa/en/
[129] http://www.domains.qa/en
[130] http://www.qu.edu.qa/students/admission/graduate/admission_requirements.php
[131] http://www.abp.edu.qa/output/page1883.asp
[132] https://www.cna-qatar.com/IT/Pages/home.aspx
[133] http://www.arabianbusiness.com/qatar-setup-cyber-security-system-489238.html
[134] http://www.newhorizons.com/LocalWeb/content/ContentOne.aspx?TemplateId=6648&GroupId=318

1.11.3 Base industrielle et technologique

Le Qatar connait l'une des plus fortes croissances au niveau mondial, ce qui en fait un pays attractif.

Le Qatar fait de la technologie et du savoir des « outils stratégiques » pour son développement[135]. C'est pourquoi le pays s'efforce de renforcer ses investissements dans le secteur. Une posture concrétisée par le projet Qatar National Vision 2030. Objectif : « atteindre les mêmes niveaux de connectivité que les pays développés »[136].

Le Qatar accorde une place importante aux jeunes entreprises dans le secteur des technologies de l'information et de la communication. L'exemple le plus parlant étant son incubateur, le « Parc des Sciences et des Technologies du Qatar », proposant des programmes de soutien et aidant les entreprises à commercialiser leurs produits. Parmi les entreprises déjà membre, peuvent être citées EADS, ExxonMobil, General Electric, Microsoft, Shell ou encore Total.

Avec de tels incubateurs, le Qatar souhaite apparaitre comme une destination attractive pour les entrepreneurs étrangers. Des sociétés telles qu'Orange ou Cisco sont notamment impliquées dans la modernisation des villes du Qatar. Cisco participe à la « Cité des technologies de l'information et des communications ». Orange a pour sa part lancé en janvier 2013[137] une joint-venture dédiée aux grands projets d'intégration dans le pays. Baptisée EGN LLC, elle a pour objectif de « capitaliser sur les multiples opportunités du marché qatari des technologies de l'information et des télécommunications ».

Le Qatar et le Koweït investissent dans un projet de construction d'un câble Internet dans le Golfe. Leur objectif est d'offrir aux opérateurs de la zone une liaison alternative vers l'Europe afin de réduire le risque de rupture de connexion. A ce sujet, el Jawad Abbassi, directeur général de l'Arab Advisors Group à Amman, précise que les opérateurs souhaitent garder leurs câbles à l'abri de toute escalade de l'Iran, et « veulent avoir de multiples voies afin d'impliquer de multiples juridictions, en cas de complications techniques ou non techniques ». Les opérateurs souhaitent enfin réagir suite aux attaques récentes subies par RasGas Qatar[138].

[135] https://itunews.itu.int/fr/2352-La-technologie-et-le-savoir-des-outils-strategiques-pour-le-developpement.note.aspx
[136] https://itunews.itu.int/fr/2352-La-technologie-et-le-savoir-des-outils-strategiques-pour-le-developpement.note.aspx
[137] http://www.orange-business.com/fr/presse/orange-business-services-lance-une-joint-venture-au-qatar
[138] http://lobservateurdumaroc.info/wp-content/uploads/2013/03/FT_208.pdf

1.11.4 Sécurité et gouvernance des réseaux

1.11.4.1 Ecosystème cybercriminel et hacktiviste

Selon les autorités qataries, la cybercriminalité serait en baisse au Qatar depuis quelques années. En 2011, le ministère de l'intérieur aurait ainsi enregistré 158 affaires de fraude sur internet. 139 cas avaient été enregistrés en 2008, 190 en 2009 et 195 et 2010[139].

En août 2012, la société RasGas était victime d'une cyberattaque, peu de temps après l'incident relatif à la société saoudienne Saudi Aramco. Si les ordinateurs de la société RasGas ont été touchés, cela n'a pas affecté la production. Cette attaque vient toutefois démontrer que le secteur de l'énergie devient une cible privilégiée des cyberattaquants.

1.11.4.2 Cadre juridique de la lutte contre la cybercriminalité

2006 fut une année clé pour la juridiction qatarie en termes de technologies de l'information. L'ictQatar a été nommé régulateur du secteur des communications et des technologies de l'information, le monopole de Qtel a été brisé et la loi sur les télécommunications de 2006 a été promulguée[140].

Cette loi définit les cadres du marché des télécommunications au Qatar, mais prévoit également la surveillance des réseaux et les sanctions encourues pour quiconque porterait atteinte à la sécurité des réseaux, ces atteintes étant définies par la loi.

Le Qatar opère un filtrage et une censure assumés des contenus internet, concernant la pornographie, les atteintes à l'Islam et la dissidence politique dans les pays du Golfe. Les autorités qataries sont aussi soupçonnées de filtrer les contenus relevant de l'homosexualité et de la confidentialité des données[141].

La loi prévoit de lourdes peines pour quiconque porte atteinte à la sécurité des réseaux informatiques. En 2010, la *cyber crime police* a ainsi arrêté un écolier qatari accusé d'avoir piraté le compte Facebook d'un camarade. Risquant jusqu'à trois ans de prison, il a été condamné à un an de prison et à payer un amende de 10 000 riyal qatari (près de 2000 euros) pour ce délit. Les autorités prononcent volontairement de très lourdes peines afin de dissuader les cybercriminels[142].

Le Qatar dispose d'un CERT basé à Doha[143]. De plus, le pays souhaite développer un centre de cybersécurité doté d'un système de lutte contre la cybercriminalité. Le ministère de l'intérieur

[139] http://thepeninsulaqatar.com/qatar/208280-police-crack-158-cyber-crime-cases.html
[140] http://www.ictqatar.qa/en/type/legislation-regulation-and-decisions
[141] https://opennet.net/research/profiles/qatar
[142] http://www.thepeninsulaqatar.com/qatar/129529-cybercrime-lands-schoolboy-in-prison.html
[143] http://www.first.org/members/teams/q-cert

travaille sur ce projet et souhaite développer un nouveau cadre législatif et des infrastructures informatiques à même de contrer la cybercriminalité[144].

1.11.5 Capacité de lutte informatique

Le Qatar, comme d'autres pays du golfe, a récemment pris conscience du besoin de développer des capacités de cyberdéfense.

Le pays mène donc une réflexion en ce sens, qui n'a pas débouché sur une doctrine mais sur l'organisation d'événements de cyberdéfense tels que le *Connect Arab Summit* tenu au Qatar en 2012 et rassemblant des chefs d'Etats arabes. Plusieurs recommandations y ont été formulées, dont la création de stratégies nationales de cybersécurité dans les pays arabes sous cinq ans[145].

Le Qatar travaille donc à court terme sur l'élaboration d'une stratégie nationale et probablement d'une doctrine militaire, dépassant les simples préoccupations de protection des réseaux nationaux.

En effet, le Qatar a lancé un appel début 2013 au développement d'un centre de cyberguerre avec l'aide de partenaires privés[146]. Ce centre sera chargé d'assurer la protection des systèmes de défense et de mener la contre-attaque en cas d'intrusion, attaque ou perturbation des réseaux militaires qataris.

[144] http://www.arabianbusiness.com/qatar-setup-cyber-security-system-489238.html
[145] http://www.itu.int/ITU-D/connect/arabstates/
[146] http://www.youtube.com/watch?v=xOS5INqcRac