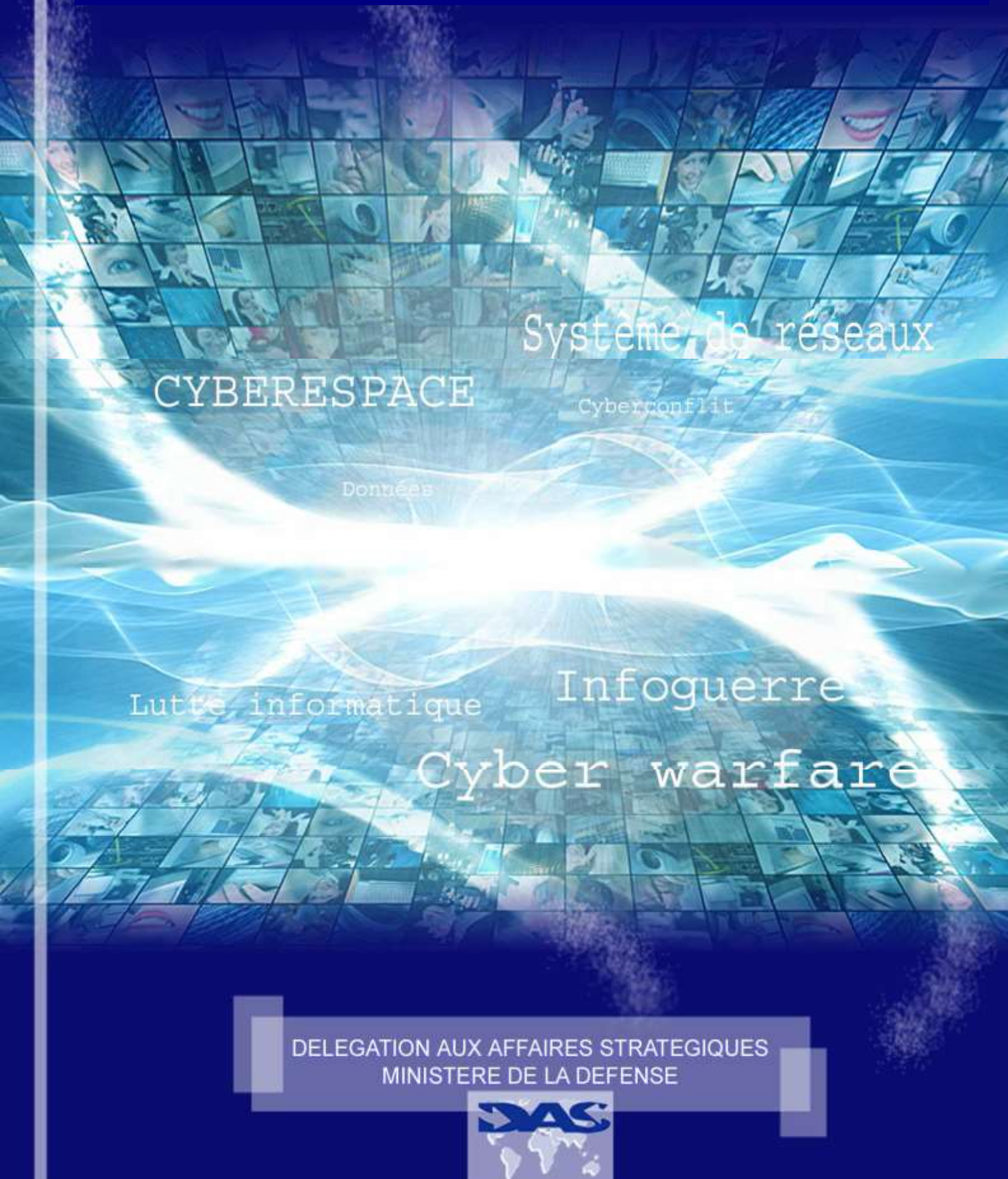
Observatoire du Monde Cybernétique
Trimestriel

Décembre 2014



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.

Table des matières

1. Fiche pays : Singapour

Singapour fait partie des pays les plus connectés au monde et constitue un véritable hub résilient pour le trafic Internet transpacifique. Le gouvernement singapourien investit beaucoup en matière de R&D. Le pays dispose d'une base industrielle forte traditionnellement spécialisée dans la production de hardware mais tendant à se développer dans le logiciel par une stratégie d'acquisition ciblée.

Signataire de la Convention de Budapest, Singapour possède une législation assez dure pénalisant la création et la distribution de virus informatiques. L'écosystème cybercriminel apparaît comme faible mais le pays est rapidement devenu une cible de choix pour des actions hacktivistes provenant de Chine et de Corée du Nord notamment.

Contraint par sa constitution de rester dans le cadre d'une action simplement défensive, Singapour a annoncé en 2014 le lancement du National Cyber Security Master plan 2018. Singapour a également élaboré une doctrine en matière cyber : le pays considère avoir le droit de répondre à une cyberattaque, cela entrant dans le cadre de leur dynamique défensive, dès lors que la cyberattaque fait partie d'une attaque armée plus classique.

1.1 Etat des lieux des infrastructures

1.1.1 *Numérisation de la société*

Au 31 décembre 2013, le pays comptait 4 millions d'internautes, soit un taux de pénétration Internet de 73 %[1]. Le taux de pénétration de l'internet haut débit était de 104,2% en 2011[2]. Au 31 décembre 2012, le pays comptait presque 3 millions d'utilisateurs Facebook, révélant une bonne pénétration des réseaux sociaux. Au fil des ans, le gouvernement de Singapour a fait la promotion de l'utilisation de l'accès Internet haut débit, dans le cadre de son programme Intelligent Nation 2015 de l'initiative (iN2015)[3]. Le service sans fil 3G a été lancé en février 2005. Le prix moyen de la connexion Internet mensuelle à Singapour est de 50 dollars[4] contre 90 dollars aux Etats-Unis.

[1] http://www.internetworldstats.com/asia.htm#sg
[2] http://en.wikipedia.org/wiki/Internet_in_Singapore#Dial-up_access
[3] http://en.wikipedia.org/wiki/Internet_in_Singapore#Dial-up_access
[4] http://www.guidemesingapore.com/relocation/introduction/singapore-cost-of-living

L'ONU effectue chaque année un classement mondial des e-gouvernements selon la qualité des services proposés. Singapour se retrouve en première position mondiale pour 2013. Une première place qu'elle détenait déjà en 2009, 2010 et 2011[5]. En 2011, 93% des utilisateurs des services de l'e-gouvernement étaient satisfaits[6]. Singapour a gagné son titre grâce à la fiabilité de son réseau et de ses infrastructures internet, qui constitue la première condition à l'accès aux services en ligne ainsi que la promotion des services du gouvernement en ligne. Par ailleurs, l'hyper connectivité de Singapour représente une aubaine pour le secteur de la e-santé. Les nouvelles technologies étant fortement présentes dans ce pays à la pointe de la modernité (smartphones, objets connectés etc.), de plus en plus de projets soutenus par le Gouvernement singapourien de type E-Santé voient le jour. Le budget de la santé représente aujourd'hui 4,1 milliards d'euros. De nombreux projets sont menés dans la santé pour améliorer la productivité et baisser les coûts des soins : les smartphones peuvent par exemple être très utiles aux patients souffrant de diabète grâce à des applications spécialement conçues pour leur facilité la vie. Cette politique devrait inciter les entreprises à continuer à s'implanter à Singapour. Cependant, toutes les technologies doivent être validées par la Health Service Authority et cela peut prendre entre 6 mois et 1 an[7].

1.1.2 *Connectivité*

Nombre de points d'échange Internet (IXP)	6[8]
Liste de points d'échange Internet (IXP)	Changi North, Tuas, Sakra Island, Tabah Merah, Katong, Singapore[9]
Nombre de datacenters	21[10]
Nombre d'Autonomous Systems	1[11]
Nombre de serveurs DNS	6[12]
Nombre de FAI	<10
Liste de FAI	SingTel, StarHub, My Republic, Mobile One[13], Qmax Communications, SingTel Data3, etc.

[5] http://www.cefrio.qc.ca/veille-strategique/intervention-citoyenne-services-publics/gouvernements-en-ligne-singapour-toujours-premiere/

[6] http://workspace.unpan.org/sites/Internet/Documents/UNPAN90601.pdf

[7] http://www.ubifrance.fr/singapour/001B1401508A+singapour-l-hyper-connectivite-de-singapour-une-aubaine-pour-le-secteur-de-.html

[8] http://www.submarinecablemap.com/#/

[9] http://www.submarinecablemap.com/#/

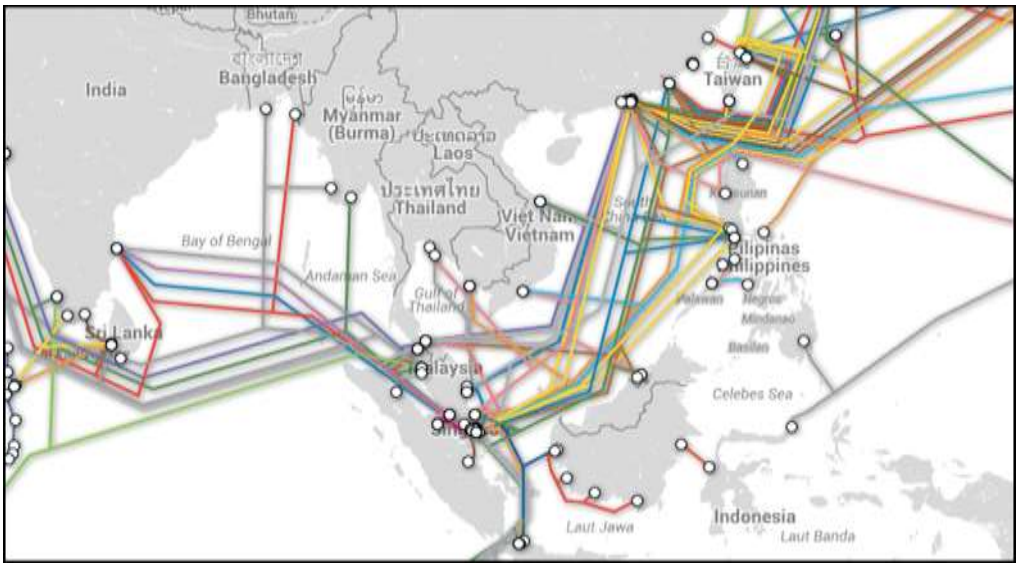
[10] http://www.datacentermap.com/singapore/singapore/

[11] http://www-public.it-sudparis.eu/~maigron/RIR_Stats/RIR_Delegations/ARIN/ASN-Alpha.html

[12] http://www.root-servers.org/

[13] SingNet, StarHub, et M1

Nom du domaine	.sg[14]
Nombre de noms de domaines	110 000 en 2009[15]
Nombre de câbles sous-marin	20
Noms des câbles sous-marins	Batam-Regit Cable System (BRCS), APX-West, Asia-Africa Europe-1 (AAE-1), Asia-America Gateway (AAG) Cable System, etc.



Submarine Cable Map[16]

1.1.3 *Perspectives*

1.1.3.1 Projet de « Smart Nation »

Le gouvernement de Singapour souhaite transformer le pays en « Smart Nation », où les secteurs tels que l'info-communication et les média peuvent prospérer grâce à une hyper connectivité[17] et une meilleure utilisation du Big Data. Le pays a déjà un fort taux de connectivité. Pour continuer à prospérer, Singapour a besoin d'investir dans l'infrastructure digitale[18].

---

[14] https://www.cia.gov/library/publications/the-world-factbook/geos/sn.html

[15] http://www.register.be/fr/nom-de-domaine/sg/Singapour-enregistrez-votre-nom-de-domaine.asp

[16] http://www.submarinecablemap.com/#/

[17] http://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/iN2015/IDAInfographi.pdf

[18] https://blog.schneider-electric.fr/datacenters/2014/10/15/les-data-centers-sollicites-smart-nation-hyper-connecte/

1.1.3.2 Construction d'un câble sous-marin Marseille-Singapour

Orange a annoncé en juillet 2014 la signature d'un accord avec une douzaine de partenaires du secteur, dont SingTel en vue de construire un nouveau câble sous-marin entre la France et Singapour. Baptisé Sea-Me-We 5 (South East Asia-Middle East-Western Europe 5), long d'environ 20 000 km, ce câble sera mis en service en 2016[19].

1.2 Capacités scientifiques et techniques

La R&D est devenue la pierre angulaire de la stratégie économique du pays. D'ici à 2015, Singapour entend accroître ses dépenses brutes dans ce domaine pour atteindre 3,5% du produit intérieur brut (PIB). Le secteur tertiaire du pays – ses universités, instituts de recherche et écoles supérieures – joue un rôle clé en matière d'incubation. Singapour possède 15 laboratoires pour l'ingénierie, les technologies de l'information et de la communication, l'informatique et les médias numériques et interactifs.

Sur 5 ans, Singapour souhaite allouer 130 millions de dollars à la recherche sur les aspects technologiques et humains de la cybersécurité. La recherche portera également sur des études plus stratégiques, portant sur la gouvernance Internet et la définition de politiques générales de sécurité. Dans son étude intitulée « Critical Times Demand Critical Skills », le cabinet Frost & Sullivan, appuyé par Booz Allen Hamilton, indique d'ailleurs que la demande en « security strategist » serait plus élevée que la moyenne à Singapour[20].

[19] http://www.maritima.info/depeches/economie/marseille/29293/construction-d-un-cable-sous-marin-marseille-singapour.html

[20] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/GISWS-Skills-Gap-Analysis.pdf

1.2.1 *Laboratoires*

Listes des universités et écoles proposant des formations en informatique	Nayang Technological University (NTU), National University of Singapore (NUS), Singapore Management University (SMU), Singapore Polytechnic[21]
Centres de recherches	Science Computer Based Learning Centre (CBLC)[22] ; East Asian Institute ; Agence for Science, Technology and Resaerch (A*STAR) ; Data Storage Institute (DSI) ; INFINITUS ; TL@NUS

Le centre de recherche Incofomm center for excellence (INFINITUS) de la Nanyang Technological University héberge plusieurs laboratoires, dont un dédié à la sécurité. Les travaux portent sur l'analyse cryptographique, la biométrie ou encore la sécurité réseaux.[23]

Les Temasek Laboratories (TL@NUS), lancés en 2000 par le ministère de la Défense singapourien avec la National University of Singapore, mènent des recherches dans les domaines de la sécurité et de la défense, notamment sur la sécurité de l'information (sécurité des technologies sans fil, chiffrement, sécurité des systèmes d'exploitation).[24]

Le CAIS (Centre for Advances Information Systems) pilote des travaux sur la gestion des données, la santé du futur, la sécurité et la confidentialité des données au sein de la Nanyang Technological University.[25]

Le ForSe Lab (Forensics and Security Lab) mène depuis 2005, au sein de la Nanyang Technological University (NTU), des travaux de recherche appliquée en sécurité informatique et analyse des données.[26]

Le CNL (Communication and Network Laboratory) est un laboratoire de recherche de la National University of Singapore. Il est principalement porté sur la sécurité des réseaux de communication.[27]

Le DSI (Data Storage Institute) développe de nouvelles technologies de stockage en intégrant la problématique de la sécurité et de l'intégrité des données.[28]

---

[21] http://fr.slideshare.net/yan2506/smm13-007

[22] http://www.cirs-tm.org/org-fr.php?pays=Singapour&matiere=infor

[23] http://www.infinitus.eee.ntu.edu.sg/

[24] http://www.temasek-lab.nus.edu.sg/program/program_info.php

[25] http://www.cais.ntu.edu.sg/content/overview/mission.jsp

[26] http://www3.ntu.edu.sg/SCE/labs/forse/

[27] http://cnl-ece.nus.edu.sg/

L'Institute for Infocomm Research (I²R) fait partie d'A*STAR et participe à la recherché en matière de sécurité, de cryptographie, de gestion des données.[29]

Le projet iCity Lab travaille sur les problématiques liées aux villes intelligentes, en s'attachant particulièrement aux questions de sécurité et de vie privée.

1.2.2 *Main d'œuvre*

Singapour souffre déjà du manque de ressources et de main-d'œuvre. La ville doit compter sur les travailleurs et investissements étrangers pour rester compétitive face à des concurrents tels que l'Inde, la Chine ou d'autres nations. Son principal problème consiste à trouver et à conserver des ingénieurs qualifiés. Cette pénurie est aggravée par des salaires peu attractifs. A Singapour, les meilleurs ingénieurs travaillent dans la finance ou dans le secteur public, ou partent dans les pays voisins, comme la Chine. A l'heure actuelle, la demande en ingénieur IT s'élève à plus de 1000[30], et ce nombre continuera d'augmenter dans les années à venir. En 2013, le nombre de professionnels de la cybersécurité ne dépassait pas 1% de la totalité des professionnels du secteur de l'IT.

Pour développer la main-d'œuvre qualifiée, l'un des projets du gouvernement singapourien est de proposer de nouvelles formations dans les universités. L'Institut de technologie de Singapour, par exemple, va lancer le premier programme de baccalauréat avec une spécialité « sécurité de l'information » en septembre 2015. Dès l'année prochaine, plus de 30 bourses d'études postuniversitaires seront également distribuées pour ceux qui souhaitent poursuivre leurs études et de mener des recherches en matière de cybersécurité. Des écoles telles que Singapore Polytechnic's Cyber Security Academy, Singapore Technologies Electronics, Engineering's DigiSAFE Cyber Security Centre offriront des possibilités de formation[31].

1.2.3 *L'entrainement et la formation professionnelle*

Le programme « Company-Led Training » (CLT) a été initié par l'IDA, afin d'améliorer l'entrainement et la formation des jeunes professionnels dans le secteur de la cybersécurité. Pour aller plus loin, le DigiSafe Cyber Security Centre ouvert en juin 2014 propose un entrainement très poussé et opérationnel en cybersécurité. Cet entrainement prépare à la détection et à la réponse aux cyberattaques dans des situations réalistes.

---

[28] http://www.dsi.a-star.edu.sg/

[29] http://www.i2r.a-star.edu.sg/

[30] http://www.psb-academy.edu.sg/column/engineers-in-demand-in-singapore/

[31] http://www.ida.gov.sg/blog/insg/talent/strengthening-singapores-cybersecurity/

1.2.4 *Perspectives*

Singapour lance par ailleurs régulièrement des challenges informatiques afin d'identifier les nouveaux talents[32].

Classement des universités technologiques de Singapour au niveau international	13ème : National University of Singapore (NUS) 33ème : Nanyang Technological University (NTU)[33]
Organisation de salons	Décembre 2014 : Asia-Pacific Security Forum & Exhibition[34], Singtal Cyber Security Forum 2012 : Joint Cyber Security Forum Asia[35]

En 2013, on note enfin que le groupe israélien IAI a ouvert à Singapour un centre de Recherche et Développement spécialisé dans la cybersécurité, ce qui lui permet de disposer d'une porte d'accès privilégiée aux marchés asiatiques[36].

1.3 Base industrielle et technologique

Le marché de la cybersécurité singapourien devrait largement progresser dans les prochaines années Singapour est vue comme un hub essentiel dans la région Asie-Pacifique.[37]

[32] https://www.gosafeonline.sg/NISEC ; www.codextremeapps.org ; http://nsc.sp.edu.sg/2014/ ; http://nsc.sp.edu.sg/2014/ ; http://www.nyp.edu.sg/sgcc ; http://www.nyp.edu.sg/i.code ; http://bit.ly/SSTMakeAthon ; http://www.academymetriders.com/index.php ; https://www.infopier.sg/scssplashawards

[33] http://www.timeshighereducation.co.uk/world-university-rankings/2013-14/subject-ranking/subject/engineering-and-IT

[34]https://www.asisonline.org/Education-Events/Global-Conferences/Asia-Pacific-Security-Forum-Exhibition2014/Pages/default.aspx

[35] http://www.asiapacificsecuritymagazine.com/join-cyber-security-forum-asia-in-singapore/

[36] http://www.israelvalley.com/news/2014/02/16/42516/cyber-security-une-premiere-iai-ouvre-un-r-d-center-a-singapour

[37] http://www.zdnet.com/article/data-analytics-growth-will-fuel-singapore-cybersecurity-market/

1.3.1 *Industrie hardware*

En 2012, l'industrie microélectronique singapourienne représente 27 % du produit intérieur brut, l'électronique 29,5 % de la production industrielle globale et les semi-conducteurs 48 % de la production électronique. En 2013, le secteur électronique représente 30% de la production manufacturière qui, à son tour, compte pour 28% dans le PIB du pays[38]. L'emploi pour l'industrie hardware s'élève à 80 000, soit 19% des emplois totaux dans l'industrie IT. En outre, la fabrication de produits électroniques crée de nombreuses retombées pour d'autres segments de l'économie, tels que les fabricants de composants, les produits chimiques et les fournisseurs de matériaux[39]. Singapour abrite 14 usines de production de semi-conducteurs, 20 usines de test et d'assemblage et 40 centres de design regroupant 1 000 designers. Le secteur emploie ainsi 40 000 personnes. Avec 10 % des parts du marché mondial pour la production de semi-conducteurs, la ville-Etat de Singapour est le 6ème pays producteur de composants électroniques[40].

1.3.2 *Industrie logicielle*

L'industrie logicielle singapourienne est dominée par les multinationales américaines telles qu'IBM ou Oracle. Des acteurs français tels que Gemalto, Adixen ou SOITEC sont également présents.

1.3.3 *Technologies de l'Information et de la Communication (TIC)*

Les TIC sont un pilier de l'économie singapourienne, avec un chiffre d'affaires de 26 milliards d'euros pour l'informatique et les télécommunications et 34 milliards pour l'électronique. Pour la période 2011-2015, le nouveau plan de financement de la recherche annoncé par le Premier Ministre s'élève à 16,1 milliards de dollars, soit 20% de plus que le précédent budget quinquennal[41].

L'autorité de régulation du marché des TIC est l'Infocomm Development Authority (IDA). Elle exerce un fort pouvoir décisionnel sur le développement des marchés du secteur de l'Internet et des télécommunications. Elle propose des aides financières aux différents acteurs locaux et internationaux.

Le gouvernement a lancé en juin 2005 un plan de développement intitulé iN2015 (Intelligent Nation 2015) qui s'est donné pour objectifs une amélioration des infrastructures et le développement renforcé des compétences techniques locales[42]. Dans le domaine des TIC, les secteurs suivants sont

---

[38] http://fr.slideshare.net/yan2506/smm13-007
[39] http://www.senat.fr/rap/r07-417/r07-41729.html
[40] http://www.senat.fr/rap/r07-417/r07-41729.html
[41] http://fr.slideshare.net/yan2506/smm13-007
[42] http://fr.slideshare.net/yan2506/smm13-007

particulièrement porteurs : Cloud Computing, services de géo localisation, médias numériques, paiements mobiles, TIC appliqués au domaine de la santé. 865 millions d'euros d'appels d'offres publics ont été lancés en 2009 dans les TIC, pour près de 400 projets, notamment pour la protection des systèmes informatiques et des données gouvernementales[43].

1.3.4 *Politique d'innovation*

Depuis les années 2000, le gouvernement singapourien a mis en place un certain nombre de dispositifs pour attirer les entreprises innovantes. Ainsi, les incubateurs de startups singapouriennes sont soutenus par le Technology Incubation Scheme (TIS), qui fait partie de la National Research Foundation (NRF), une agence gouvernementale créée en 2006 pour développer la R&D de Singapour. Singapour constitue donc un environnement très propice pour les entrepreneurs du numérique de tous horizons. Son dynamisme attire également des grands noms de la haute technologie, qui ont installé des filiales à Singapour ces dernières années : Groupon, Apple, IBM, mais aussi Microsoft, Samsung, Facebook et Google. C'est en 2007 que Google a installé ses bureaux à Singapour. Fin 2011, la firme a investi 120 millions de dollars dans un nouveau centre de données : il s'agit du troisième Datacenter de Google en Asie, après celui de Hong-Kong et celui de Taïwan[44].

1.4 Ecosystème cybercriminel et hacktiviste

1.4.1 *Ecosystème cybercriminel*

L'impact financier de la cybercriminalité sur Singapour s'élèverait à plus de 1,25 milliards de dollars en 2013[45]. Les cybercriminels ont par exemple piraté les réseaux d'entreprises, les banques centrales et le ministère des finances pour acquérir des informations à des fins de manipulation financière[46].

L'ASEAN est l'une des zones les plus touchées par la cybercriminalité. Alors que les pertes occasionnées à Singapour représentent 0,41% de son PIB, la sécurité des données devient

[43] http://fr.slideshare.net/yan2506/smm13-007

[44] http://fr.slideshare.net/yan2506/smm13-007

[45] http://www.techgoondu.com/2014/06/11/report-cyber-crime-costs-singapore-an-estimated-s1-25bn-annually/#.VIh3IXuApmV

[46] http://www.techgoondu.com/2014/06/11/report-cyber-crime-costs-singapore-an-estimated-s1-25bn-annually/#.VIh3IXuApmV

impérative. Les problèmes majeurs reposent sur la formation du personnel en matière de sécurité, la méconnaissance des outils et le manque de moyens[47].

Selon un rapport d'enquête de fraude du cabinet d'audit, KPMG Singapour, entre 2004 et 2008, le nombre de cyberattaques contre les entreprises a augmenté de 40%. Singapour est le deuxième pays le plus visé par des attaques informatiques d'intimidation après les Etats-Unis. En 2006, 25% des 3488 étudiants Singapouriens interrogés ont déclaré avoir été victimes de cyberattaques[48].

Si le pays est régulièrement la cible d'attaques informatiques, il est en revanche rarement à l'origine des menaces. Selon une étude réalisée par la société Sophos en 2008, le nombre de malwares produits par les cybercriminels singapouriens s'élèvent à 0.1%, contre 37% pour les Etats-Unis. Le nombre de spams s'élève à 0.3% contre 17,5% pour les Etats-Unis[49].

1.4.2 *Ecosystème hacktiviste*

En 2013, près de 180 sites internet singapouriens ont été victimes de deux vagues successives d'attaques informatiques. Parmi eux, plusieurs sites du Reform Party, un parti d'opposition créé en 2008 par Kenneth Jeyaretnam, qui prône la mise en place d'une réelle démocratie dans la cité Etat. Un drapeau indonésien sur lequel était inscrit le mot Looser était affiché sur la page d'accueil du site. Une attaque revendiquée par un groupe auto-baptisé Anonymous Indonesia.

La même année, le groupe hacktiviste Anonymous et le hacker « le Messie » avaient réussi à prendre le contrôle de plusieurs sites ministériels. Environ 19 sites gouvernementaux avaient subi une attaque par déni de service. Le site Yahoo Singapore avait été aussi l'objet d'attaque[50]. En conséquence, Singapour a relevé son niveau d'alerte cyber et renforcé la protection de ses systèmes d'information[51].

---

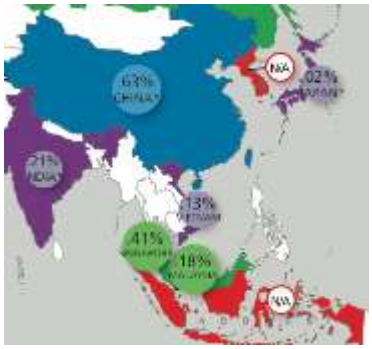
[47] UBIFRANCE organisera du 14 au 21 avril 2015 à Hanoi un colloque sur la cybersécurité, où seront présents des représentants du gouvernement singapouriens (http://www.ubifrance.fr/programme-france/001PRG-22377+colloque-sur-la-cybersecurite-singapour-malaisie-vietnam.html)

[48] http://www.academia.edu/406791/Analysis_of_Computer_Crime_In_Singapore_Using_Local_English_Newspapers

[49] http://www.academia.edu/406791/Analysis_of_Computer_Crime_In_Singapore_Using_Local_English_Newspapers

[50] https://sg.news.yahoo.com/hacker--the-messiah--claims-attack-on-singapore-govt-sites--repeats-%E2%80%98anonymous%E2%80%99-cyber-threat-090023141.html

[51] http://www.courrierinternational.com/article/2014/02/20/attaques-ciblees-sur-singapour



Coût de la cybercriminalité sur le PBI

1.5 Organisation de la cybersécurité

1.5.1 *A l'échelle nationale*

1.5.1.1 Régulation internet

Le gouvernement de Singapour fait souvent la une des médias en raison des restrictions de la liberté d'expression sur Internet. Tout comme la Malaisie ou la Birmanie, le gouvernement de Singapour lutte en effet activement contre l'intolérance raciale, la diffamation et les propos déformés visant tant l'image officielle que la situation financière des personnalités politiques. A Singapour, les services Internet sont ainsi soumis à la réglementation de l'Autorité de développement des médias (MDA) qui bloquent des sites à contenu pornographique, comme Playboy, YouPorn et PornHub. Depuis Juillet 2014, 45 sites de piratage tels que The Pirate Bay et KickassTorrents, ont tous été bloqués[52].

1.5.1.2 Arsenal législatif

1.5.1.2.1 Le Computer Misuse Act

En 1993, Singapour a adopté la Loi *Computer Misuse Act* qui traite de crimes informatiques et prévoit des sanctions sévères en cas de violation. Mais la définition de la cybercriminalité était encore floue : le gouvernement a pu par exemple appliquer des dispositions du Code pénal général à des activités qui pourraient entrer dans le champ de la cybercriminalité. Par exemple, une cyberattaque à l'aide

[52] http://en.wikipedia.org/wiki/Internet_censorship_in_Singapore

d'un malware serait jugé en vertu de la Loi Computer Misuse, alors un crime économique serait sous l'égide du Code pénal[53].

1.5.1.2.2 Le Spam Control Act

Une loi anti-spam a été adoptée par le Parlement de Singapour en 2007. Cette loi prévoit le contrôle du spam dans les échanges informatiques et téléphoniques.

1.5.1.2.3 La Computer Misuse and Cybersecurity Act (CMCA)

Le 14 janvier 2013, la loi fut rebaptisée *Computer Misuse and Cybersecurity Act* (CMCA) et permet désormais au ministère de l'Intérieur de prendre des mesures préventives pour prévenir, détecter et menaces de cyberattaques pouvant affecter les communications de Singapour, les infrastructures, les transports, les services bancaires et financiers, les services publics, les transports en commun, les services de police, la défense civile et les services de santé.

1.5.1.2.4 Mise en œuvre

La plupart des dispositions de la Loi *Computer Misuse Act* sont passibles d'une amende maximale pouvant aller jusqu'à 10 000 dollars singapouriens et / ou 3 ans d'emprisonnement pour une première infraction. Pour les cas de récidive, la peine est une amende allant jusqu'à 50 000 dollars singapouriens et / ou 7 ans emprisonnement. Si les cyberattaques visent les services bancaires, financiers ou les communications, la peine peut aller jusqu'à 100 000 dollars singapouriens et / ou 20 ans d'emprisonnement[54].

1.5.1.3 Protection des infrastructures

En octobre 2013, Singapour a dévoilé un plan prévoyant 130 millions de dollars sur 5 ans pour améliorer les capacités de protection, de défense et de réaction de la Nation face à la montée en puissance des cyberattaques[55].

Le 24 juillet 2014, le gouvernement de Singapour lançait le projet National Cyber Security Masterplan 2018, une version améliorée des plans Infocomm Security Masterplan et Infocomm Security Masterplan 2, initiés respectivement en 2005 et 2012. Ce plan prévoit l'amélioration de la sécurité et la résilience des infrastructures critiques, le renforcement des capacités de détection et d'analyse des menaces cyber, missions déjà menées par le Cyber Watch Centre et le Threat Assessment Centre.

---

[53] http://maplesecrets.blogspot.fr/2011/08/singapore-law-on-cyber-crime-eg-hacking.html

[54] http://maplesecrets.blogspot.fr/2011/08/singapore-law-on-cyber-crime-eg-hacking.html

[55] http://news.asiaone.com/news/singapore/singapores-cyber-defence-firepower-gets-130m-boost

Pour les objets connectés et réseaux intelligents, Singapour a mis en place l'Ambient Networks Secure Eco System. Cette initiative a pour objectif de sécuriser les réseaux intelligents en proposant des standards d sécurité et de conformité.

1.5.1.4 Partenariats public-privé

Dans le cadre des efforts continus pour améliorer la protection des réseaux informatiques et les réponses aux cyberattaques, le gouvernement travaillera en étroite collaboration avec le secteur privé au sein de plusieurs exercices de cybersécurité.

- Le Critical infocomm Infrastrcuture (CII) Protection Asessment programme vise à évaluer la sécurité des systèmes informatiques.
- Le National Cyber Security Exercise programme vise à améliorer la capacité de réponse aux cyberattaques au niveau national. Le programme envisage la mise en place de plusieurs exercices de cybersécurité nationaux et régionaux.

Le NCSM2018 vise également à faciliter le partage d'informations entre le gouvernement et le secteur privé, pour promouvoir la sécurité et l'échange d'informations sur les cybermenaces.

1.5.1.5 Acteurs

Singapour dispose d'un CERT national, le SingCERT.

L'agence nationale en charge de la cybersécurité est le Singapore Infocomm Technology Security Authority (SITSA). La mission du SITSA est de sécuriser l'environnement IT du pays, d'anticiper les menaces informatiques telles que le cyberterrorisme ou le cyberespionnage. Cette agence a été inaugurée le 1er octobre 2009. Elle est en charge de superviser l'implémentation des mesures de sécurité auprès des infrastructures critiques à l'échelle nationale, les autorités sectorielles restant responsable à l'échelle de leur propre secteur. Le SITSA dispose de son propre CIRT, le SITSA IRT[56].

La SITSA est dirigée depuis 2009 par Ng Hoo Ming et est structurellement positionnée au sein du Département de la sécurité interne (ISD) du ministère des affaires intérieures singapourien.

Avec le lancement en 2014 du National Cyber Security Masterplan 2018[57], Singapour poursuit sa logique de centralisation des différentes agences en créant le NISC, le National Infocomm Security Committee. Ce comité est composé de membres de plusieurs agences gouvernementales :

---

[56] http://www.first.org/members/teams/sitsa_irt

[57] http://www.ida.gov.sg/~/media/Files/Collaboration%20Initiatives/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf

- A*STAR, (Agency for Science, Technology and Research)
- IDA (Infocomm Development Authority of Singapore)
- MCI (Ministry of Communications and Information)
- MHA (Ministry of Home Affairs)
- MINDEF (Ministry of Defence)
- MOF (Ministry of Finance)
- NSCS (National Security Coordination Secretariat)
- NRF (National Research Foundation)

Ce nouveau comité a pour mission de formuler les orientations stratégiques du pays en matière de cybersécurité, et de guider le développement et l'implémentation des mesures de sécurité émises par le National Cyber Security Masterplan 2018.

Lors du séminaire Infocomm Sécurité du 26 août 2014, le ministre des communications et de l'information singapourien, le Dr Yaacob Ibrahim, a déclaré qu'un centre de suivi et de contrôle des opérations (MOCC) sera mis en place. Le MOCC complétera le Cyber-Watch Centre (CAC). Créé en 2007 par l'IDA, il est appelé à être renforcé en janvier 2015[58] avec de nouvelles capacités de monitoring de sites web, détection, de protection contre les fuites d'information et de protection contre les malwares. Le Cyber Watch Center (CWC) fournira un large éventail de capacités de détection pour les agences gouvernementales avec l'amélioration des capacités de corrélation.

Le Threat Analysis Centre (TAC) identifie et évalue les cybermenaces et fournit aux organismes publics une analyse détaillée des cybermenaces, ainsi que des recommandations techniques.

1.5.2 *A l'échelle internationale*

1.5.2.1 Coopération régionale

Afin de contrer les cybermenaces à l'échelle régionale, l'ASEAN a créé le conseil *ASEAN Telecommunications Regulators Council* chargé de lutter contre la cybercriminalité dans les Etats membres de l'ASEAN et de renforcer la coopération. Le 11 octobre 2001 à Singapour, les ministres responsables de sécurité et de la défense ont convenu d'inclure la cybercriminalité dans le programme de lutte contre le crime transnational[59]. Le 14 janvier 2011, la *ASEAN ICT Masterplan 2015* (AIM2015) a été adopté lors du Xème sommet TELMIN qui se tenait à Kuala Lampur. Les principaux objectifs de ce programme sont le renforcement de la cybersécurité régionale, notamment entre les CERTs des différents pays membres, et la sensibilisation de la population sur la cybersécurité. Les dirigeants ont affiché leur volonté de créer l'ASEAN Network Security Action

[58] http://www.ida.gov.sg/blog/insg/talent/strengthening-singapores-cybersecurity/

[59] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Workshop1/ASEAN%27s_Cooperation_on_Cybercrime_and_Cybersecurity.pdf

Council, visant à promouvoir la coopération régionale et l'échange d'expertises en cybersécurité. Le 17 septembre 2013, à Vientiane, au Laos, les ministres ont créé le *Senior Officers Meeting on Transnational Crime* (SOMTC), visant à renforcer les liens de défense entre les pays membres. En novembre 2013, le premier ministre singapourien, Lee Hsien Loong, a enfin appelé les Etats de l'Asie du Sud Est à coopérer face à aux cybermenaces[60].

Le SingCERT coopère à l'échelle régionale avec l'APCERT, l'Asia Pacific Computer Emergency Response Team[61], le Forum FIRST[62], l'ASEAN CERT Incident Drill (ACID) et le Groupe de travail collaboratif TSUBAME mené par le Japon.

1.5.2.2 Coopération internationale

En mai 2014, à l'occasion du Shangri-La Dialogue 2014, plusieurs hauts fonctionnaires de l'armée australienne, chinoise, allemand et singapourienne ont affirmé la nécessité de renforcer la coopération régionale et internationale en cyberdéfense[63].

1.5.2.2.1 Le Complexe mondial INTERPOL pour l'innovation (CMII)

Centre de recherche et développement, le Complexe mondial INTERPOL pour l'innovation (CMII) mène un travail de recherche proactif dans de nouveaux domaines et diffuse les toutes dernières technologies de formation. L'objectif est de doter les policiers du monde entier des outils et des capacités leur permettant de relever des défis toujours plus complexes et sophistiqués.

Les trois principales composantes du Complexe mondial sont

- la sécurité numérique comme le renforcement de la cybersécurité et lutte contre la cybercriminalité;
- le travail de recherche axé sur l'étude de protocoles, d'outils et de services, et sur l'analyse des tendances en matière de cyberattaques ;
- le renforcement des capacités et formation, comme la formation à la lutte anticorruption, en particulier dans le sport et enfin l'appui opérationnel et soutien aux enquêtes, notamment l'identification des nouvelles menaces criminelles telles que : la criminalité organisée

[60] http://www.securityweek.com/singapore-urges-regional-cooperation-against-hackers
[61] http://www.apcert.org/
[62] http://www.first.org/about
[63] http://www.iiss.org/en/events/shangri%20la%20dialogue/archive/2014-c20c/special-sessions-b0a1/session-2-a1fc

asiatique; la mise en place d'une nouvelle salle des opérations du Centre de commandement et de coordination vient renforcer celles déjà en place à Lyon et à Buenos Aires (Argentine)[64].

1.5.2.2.2 Boeing ouvre un centre d'analyse cyber

En 2013, Boeing a ouvert un centre de lutte contre la cybercriminalité à Singapour. Le centre a pour finalité de former et d'équiper les professionnels afin d'assurer la cybersécurité régionale de Boeing d'excellence. Ce centre est une première pour Boeing international et permettra de répondre aux demandes croissantes de la région[65].

1.5.2.2.3 Centre d'Excellence créé par FireEye

En janvier 2014, un Centre d'Excellence a été créé par FireEye, afin de renforcer son équipe d'experts en sécurité informatique. Le centre est le premier de la région Asie-Pacifique et va embaucher et former près de 100 professionnels de la sécurité cybernétique au cours des deux prochaines années, avec l'aide d'IDA de Singapour[66].

1.6 Capacités de cyberdéfense

Petit Etat de la région d'Asie du Sud-Est, Singapour dépend fortement de son environnement extérieur. Pour ce faire, sa stratégie de défense s'inscrit dans une logique de partenariats en Asie, mais aussi avec les Etats-Unis. Singapour est à une étape clé du développement de sa cyberdéfense et ne part pas de rien. Les initiatives visent en effet à centraliser, mutualiser et coordonner les ambitions et les compétences des acteurs déjà présents.

1.6.1 ***Acteurs***

En 2013, le ministre de la défense singapourien annonçait la création du Cyber Defense Operations Force Hub, unité transverse regroupant des membres de l'armée, de la Navy et de l'Air force. Ainsi, les branches de l'armée singapourienne qui travaillaient séparément sur les questions de

[64] http://www.interpol.int/fr/%C3%80-propos-d%27INTERPOL/Le-Complexe-mondial-INTERPOL-pour-l%E2%80%99innovation

[65] http://boeing.mediaroom.com/2014-09-22-Boeing-to-Open-First-Cyber-Analytics-Center-Outside-the-US-in-Singapore

[66] http://www.ubifrance.fr/001b1400525a+singapour-ida-fireeye-met-en-place-un-centre-pour-renforcer-la-securite-cybe.html

cyberdéfense peuvent désormais mutualiser leurs efforts. [67] Cette unité fut la première de ce type en Asie du Sud-Est. La nouvelle unité est chargée d'assurer la sécurité des équipements des forces de défense singapouriennes (équipement de surveillance, systèmes d'armes, logiciels et systèmes d'exploitation). Les détails des activités de la nouvelle unité singapourienne n'ont cependant pas encore été révélés. Cette unité opérera en partenariat avec l'Infocomm Technology Security Authority et proposera des rapports réguliers sur les nouvelles menaces.

Notons qu'en cas de cyberattaque majeure à l'encontre des réseaux civils singapouriens, c'est l'agence nationale en charge de la cybersécurité le Singapore Infocomm Technology Security Authority (SITSA), qui sera en charge de mener la réponse défensive à l'échelle nationale.

Singapour n'a pas d'unité de réserviste spécialistes des TIC et/ou de la cybersécurité.

1.6.2 *Budgets*

Les programmes envisagés sont le développement de pôles d'innovation autour des technologies cyber et le recrutement d'une main d'œuvre qualifiée. Le programme de cybersécurité sera financé conjointement par la National Research Foundation (NRF), le ministère de la Défense, ministère de l'Intérieur et le Secrétariat de coordination de la sécurité nationale[68].

1.6.3 *Formations, exercices et entraînements*

Les forces armées travaillent de concert avec les universités pour intégrer la sécurité des systèmes d'information dans les programmes[69].

[67] http://www.straitstimes.com/breaking-news/singapore/story/saf-sets-new-cyber-army-fight-digital-threats-20130630

[68] http://news.asiaone.com/news/singapore/singapores-cyber-defence-firepower-gets-130m-boost

[69] http://www.pinsentmasons.com/PDF/singapore_ramps_up_cybersecurity_efforts_Sept2013.pdf

2. Les monnaies virtuelles et le financement des activités illicites, risque ou opportunité stratégique pour les Etats ?

L'une des principales armes de la lutte contre le terrorisme est le ciblage des flux financiers. Toute organisation terroriste a en effet besoin de financer ses activités. Certains frais sont lourds et incompressibles, à l'image :

- du coût de la vie quotidienne,
- de l'établissement d'un système de communication (Internet, téléphones portables, cartes prépayées…),
- du coût de l'entrainement et de l'endoctrinement (professeurs, entretien des camps, armement, etc.),
- des voyages,
- des faux papiers et documents,
- de l'établissement d'une cellule de communication et de propagande, et de l'achat du matériel nécessaire (caméras, etc.),
- et surtout, de l'armement, achat de munitions, et de composants d'engins explosifs improvisés (EEI)[70].

Certaines cellules terroristes dépensent également énormément dans le caritatif et la charité, afin de légitimer socialement leur présence et leurs actions. Le ciblage du financement de tous ces éléments est donc une piste majeure de la lutte contre le terrorisme. Les Etats l'ont bien compris et gèlent régulièrement les fonds de cellules terroristes et criminelles, ralentissant ainsi la montée en puissance et le passage à l'acte. Face à cette contre-offensive des Etats, les groupes terroristes optent pour des moyens de financement moins aisés à identifier, et plus difficile à geler. Objectif : rester sous le radar du monitoring traditionnel des flux financiers en diminuant les montants des échanges, ou en adoptant des circuits complètement détachés du circuit financier traditionnel. A titre d'exemple, Al-Qaida exploite plusieurs modes de financements[71] :

- la collecte privée de fonds ;
- les organismes de charité ;
- les entreprises offshores ;
- le trafic de drogue et la criminalité cupide traditionnelle.

Au sein de cette dernière catégorie, **la cybercriminalité prend une place de plus en plus importante**. Des investigations menées par la police britannique révèlent que trois membres d'une cellule

[70] https://fr.wikipedia.org/wiki/Engin_explosif_improvis%C3%A9

[71] http://www.terrorismanalysts.com/pt/index.php/pot/article/view/113/html

terroriste planifiant une attaque sur les Etats-Unis, l'Europe et le Moyen Orient privilégiaient le carding (vol et trafic de cartes bancaires) pour financer certains de leurs frais d'organisation et de préparation. A l'aide de 110 cartes bancaires différentes, les terroristes se sont procurés systèmes GPS, lunettes de visions de nuit, tentes, sacs de couchage, couteaux ou encore téléphones, cartes prépayées et voyages. Les hommes ont également procédé à du blanchiment de fonds sur des sites de jeux en ligne ; à des activités de phishing ayant rapporté plus de 3,5 millions de $, et à la distribution massive de mails infectés de spywares afin de prendre le contrôle des ordinateurs ciblés. Les terroristes ont également utilisé internet à des fins de réseautage, recrutement et planification.[72] Cette affinité pour les nouvelles technologies se traduit par l'usage de nouveaux modes de financement, tels que les monnaies virtuelles.

1.7 Le renouveau des modes de financement terroristes

D'ordinaire déjà complexe en raison des circuits de blanchiment, le suivi des flux financiers est rendu plus difficile par des mécanismes de micro-financement renouvelé grâce aux cartes prépayées et l'usage des monnaies virtuelles. L'étude du financement des activités terroristes révèle une palette d'outils intéressants à suivre. Il a été rapporté que des groupes djihadistes syriens auraient utilisé des monnaies électroniques et les réseaux sociaux pour financer certaines opérations. [73] Des membres d'un groupe djihadiste du nord du Causase faisant partie du Front Al-Nosra ont également sollicité des donations par les réseaux sociaux en utilisant le système de paiement en ligne russe Qiwi[74].

Le cas de Daesh

Dans une publication intitulée « Bitcoin wa Sadaqat al-Jihad », traduite en « Bitcoin and the Charity of Violent Physical Struggle », Taqi'ul-Deen al-Munthir vante les mérites de la cryptomonnaie pour le financement des activités de l'Etat islamique.

"One cannot send a bank transfer to a mujahid or suspected mujahid without the kafir governments ruling today immediately being aware"

Il rappelle que la lutte contre les infidèles se manifeste également par le refus de leurs institutions, au nombre desquelles la monnaie et son circuit tiennent une place essentielle. Les finalités de l'usage de bitcoins sont nombreuses. La première est que Bitcoin peut être utile afin de se passer de la monnaie et des taxes d'un Etat considéré comme infidèle et illégitime.

---

[72] http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945.html
[73] http://www.rferl.org/content/extremists-bitcoin-isis-media-funding/26635157.html
[74] https://qiwi.com/

"So, then, does not being pleased with paying taxes to the kufar, not intending to change it, believing it to be okay, and doing it willingly, constitute kufr ?" ; « This allows our brothers stuck outside of the ardh Dawlatul-Islam to avoid government taxes ».

La seconde est de pouvoir financer le terrorisme anonymement.

« Secretly fund the mujahideen with no legal danger upon them »
"A proposed solution to this is something known as Bitcoin."

Bitcoin répond à ces exigences grâce à un fonctionnement avantageux aux yeux de l'auteur du document : la difficile traçabilité : « untrackable by kafir governments » ; et la robustesse de son réseau : « There is no point of weakness, no one can hack the entire Bitcoin system, and as long as people use Bitcoin, it will exist safely ».

Enfin, l'auteur insiste sur le rôle de l'escrow, cet intermédiaire chargé de valider les transactions en assurant la confiance entre les parties. Ce rôle, indique-t-il, pourrait être celui du juge islamique (qadi).

« Contracts used in an online marketplace could be arbitrated by third parties who judge to see if the conditions of the contracts are met. Qadis (juge islamique) could easily be introduced to this system and rule by shari'a between Muslims across al-khilafah. It solves the online marketplace issue for al-khilafah instantly, whilst giving Muslims an alternative to use until they offer hijrah. »

« Arbitrators, which could be readapted to be qadis »

Il s'agit là d'une publication isolée d'un sympathisant de Daesh. Mais les arguments avancés par l'auteur n'en sont pas moins pertinents. Le mécanisme de fonctionnement proposé par la cryptomonnaie correspond et répond parfaitement aux besoins d'une organisation terroriste, tant en matière de financement anonyme, que d'émission d'une monnaie souveraine, détachée du circuit traditionnel et convertible en dollars.

Mais son application est, dans les faits, plus complexe. Se pose d'abord la question de l'utilité de l'adoption de Bitcoin ou de toute autre cryptomonnaie. L'Etat islamique est l'organisation terroriste la plus riche qu'il soit. Elle ne manque pas de trésorerie et ne dépend pas des donations de ses sympathisants. Elle n'a donc pas, en théorie, besoin de donations en ligne. Elle établit tout de même un mécanisme de prélèvement d'impôt, mesure permettant d'asseoir sa légitimité sur une zone géographique. La mise en place d'un circuit de donations pourrait donc aller en ce sens.

Il est encore aujourd'hui impossible de confirmer ou d'infirmer l'usage de Bitcoin par l'Etat islamique. Mais un ancien site (http://khilafah.is) diffusé par de nombreux comptes Twitter directement affiliés à Daesh, proposait l'envoi de donations en bitcoins. Le site a depuis été mis hors ligne.

Si certains observateurs indiquent que Daesh n'emploie pas le Bitcoin pour ses transactions en raison de la faible communauté d'utilisateurs de bitcoins dans la zone géographique, l'hypothèse de la

création d'une cryptomonnaie propre ne peut être définitivement écartée. Dans une interview accordée au webzine Deepdotweb[75], l'auteur de l'article précédemment cité recommande à Daesh de créer sa propre cryptomonnaie, l'eDinar. Cet eDinar ne serait pas complètement autonome, comme Bitcoin, mais serait entièrement adossé au Dinar de Daesh, dont le lancement a récemment été annoncé.

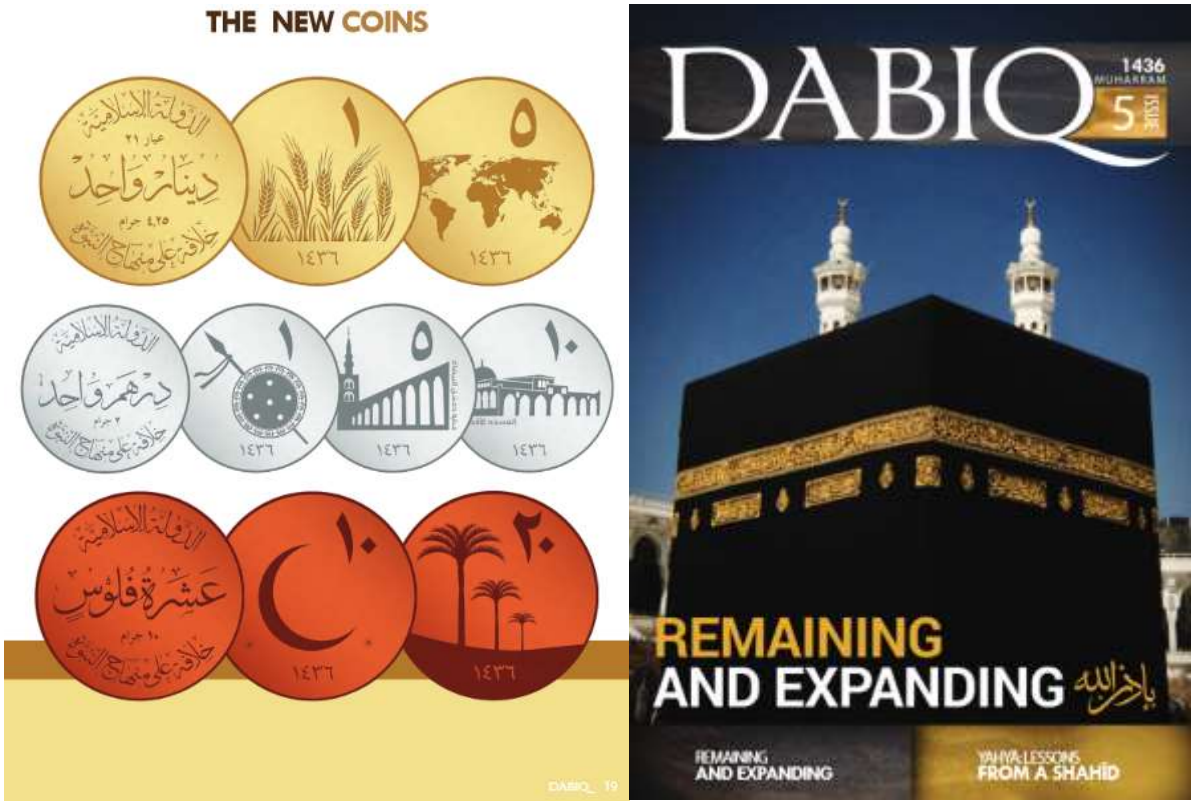


Image (gauche) extraite de l'article « THE CURRENCY OF THE KHILAFAH », Dabiq, Issue n°5 (droite)

[75] http://www.deepdotweb.com/2014/09/22/bitcoin-is-not-being-used-by-the-islamic-state/

1.8 L'investigation sur Bitcoin : une opportunité pour le suivi des transactions illicites

Les Etats sont nombreux à affirmer que le terrorisme peut potentiellement être financé par les cryptomonnaies. En février 2014 par exemple, le gouvernement canadien affirmait que le terrorisme pouvait être financé par des monnaies virtuelles telles que Bitcoin. L'Australie[76] ou encore la Russie considèrent également que Bitcoin peut être utile au financement du terrorisme. Le Département de la Défense américain a quant à lui lancé des investigations approfondies sur l'usage des monnaies virtuelles dans le financement du terrorisme.[77]

"The introduction of virtual currency will likely shape threat finance by increasing the opaqueness, transactional velocity, and overall efficiencies of terrorist attacks."

Face à ce constat, certains Etats déploient d'importants moyens afin d'identifier et de suivre à la trace les transactions illicites opérées via Bitcoin[78].

1.8.1 *L'opportunité du sentiment d'impunité*

Le fait que les transactions réalisées soient toutes stockées publiquement dans la blockchain souligne que Bitcoin n'offre pas à ses utilisateurs de l'anonymat mais du « pseudonymat ». Tout le monde peut en effet analyser, étudier les flux et transactions répertoriés dans la blockchain, et ainsi retracer la totalité des achats liés à une adresse bitcoin. Consacrant ainsi le principe du pseudonymat, Bitcoin n'est ni anonyme, ni intraçable. De ce fait, les outils d'analyse forensique de la blockchain ont rapidement émergé. A condition de disposer des outils adéquats, il est possible de retracer des transactions frauduleuses au sein de la blockchain.

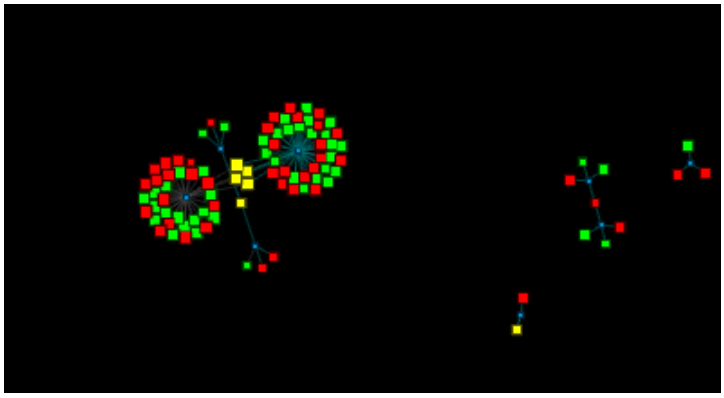
Certaines adresses bitcoins sont publiquement diffusées. L'investigation de la blockchain passe donc d'abord par la collecte en source ouverte de ces informations. Par corrélation, ces adresses peuvent être regroupées en *clusters*, et constituer un point de départ solide pour une immersion dans la blockchain. Certains outils permettront de réaliser ces agglomérations de façon automatique, grâce à

[76] http://www.heraldsun.com.au/news/law-order/organised-crime-and-addicts-using-darknet-to-trade/story-fni0fee2-1227143936100?nk=71c88d770265e55a63d89146b83d158f

[77] http://news.sky.com/story/1296508/global-jihad-could-be-funded-with-bitcoin

[78] http://www.heraldsun.com.au/news/law-order/organised-crime-and-addicts-using-darknet-to-trade/story-fni0fee2-1227143936100?nk=71c88d770265e55a63d89146b83d158f

des algorithmes dédiés. Citons, de la simple visualisation à l'analyse : Blockchain.info, Numisight[79], QuantaBytes qui propose des analyses simplifiées, Blockonomics[80] qui offre la visualisation du réseau d'un utilisateur, Bitcoin Transaction Visualization[81], CryptoCrumb[82] qui propose explicitement l'analyse forensique de la blockchain, dailyblockchain[83], BlockExplorer, Bit Force 5, Snort 987 block parser. Notons également l'existence d'un *transform* dédié à Maltego[84] [85].



Représentation de transactions de la blockchain. Source : http://dailyblockchain.github.io/

Les logiciels d'analyse de la blockchain proposeront généralement les fonctionnalités suivantes :

- Le « parser » qui lit les blocks ;
- Le « clusterizer » qui identifie des adresses et groupes d'adresses afin de les labelliser ;
- Des « crawlers » qui vont, à partir de sources ouvertes sur des forums, identifier les adresses diffusées publiquement et ainsi associer les *clusters* à des pseudonymes, entreprises ou individus.

Certains outils peuvent également utiliser des « tags » librement accessibles en ligne, et identifiant déjà quelques groupes d'adresses, dont certaines ont fait l'objet de saisies judiciaires. Des outils de visualisation présenteront toutes ces informations sous forme de graphiques. Des logiciels comme Gephi peuvent également être mis à contribution. Les algorithmes permettent d'identifier une transaction issue de plusieurs adresses bitcoin appartenant à un seul et même propriétaire, mais également les adresses fantômes. Enfin, certains outils permettent de détecter des schémas

[79] http://signup.numisight.com/
[80] http://blockonomics.co/
[81] http://bitcoin.interaqt.nl/
[82] http://signup.cryptocrumb.com/
[83] http://dailyblockchain.github.io/
[84] http://bostonlink.github.io/about/
[85] https://s3.amazonaws.com/bostonlink/Presentations/bitcoin_explorer.pdf

frauduleux[86] ou « patterns » : ils identifient les anomalies au sein des transactions recensées par blockchain (éparpillement d'un montant, utilisation d'adresses fantômes, blanchiment manuel par la création de plusieurs adresses Bitcoin…).[87]

Dans l'étude[88] intitulée « BitIodine: Extracting Intelligence from the Bitcoin Network » les auteurs relèvent d'ailleurs le défi de retracer les transactions effectuées dans le cadre de la campagne du rançongiciel CryptoLocker à partir de l'analyse de la blockchain. Les chercheurs indiquent avoir quantifié avec exactitude le nombre de rançons payées en bitcoins, et avoir collecté quelques informations sur les victimes. CryptoLocker est un rançongiciel chiffrant les données de la victime ; les cybercriminels ne libérant les données qu'en cas de paiement d'une rançon, acquittée le plus souvent en bitcoins. Avec BitIodine, il serait possible d'identifier grâce au *parser* les *clusters* d'adresses appartenant aux cybercriminels de CryptoLocker, et ainsi d'établir des statistiques sur les rançons payées.

1.8.2 *Le revers des Dark monnaies*

Dans son article, Taqi'ul-Deen al-Munthir évoque Dark Wallet, outil permettant de rendre encore plus opaques les transactions effectuées via Bitcoin. Il s'agit là d'un enjeu majeur : Bitcoin est, en l'état, traçable et non-anonyme. Son usage par les organisations terroristes et criminelles peut donc être appréhendé par les Etats qui, avec des outils de monitoring adaptés, peuvent retracer et cartographier les échanges une fois les adresses BTC identifiées. Mais les évolutions des cryptomonnaies vers plus d'opacité (suppression de l'historique « blockchain », chiffrement, blanchiment intégré) viennent indéniablement compliquer la tâche des enquêteurs.

Les utilisateurs et développeurs tendent en effet aujourd'hui vers la création de monnaies ou d'*add-ons* corrigeant l'absence d'anonymat et la traçabilité caractérisant Bitcoin. Des cryptomonnaies plus anonymes telles que BitcoinDark, DarkCoin, CloakCoin, XCurrency, ZeroCoin, FedoraCoin, CryptoNote… sont pour la plupart déjà en circulation. Le fonctionnement de ces moyens d'échange (anonymisation, nœuds de confiance, re-routage sécurisé, blanchiment intégré au protocole…) rend aujourd'hui bien plus complexe l'identification des flux illicites de monnaies virtuelles, notamment en raison de l'absence de blockchain. Ces monnaies sont toutefois – pour l'instant - moins répandues

[86] http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/

[87] A titre d'exemple, BitIodine se charge de la collecte en sources ouvertes et de l'agrégation des adresses en *clusters* uniques. Une fois ces *clusters* identifiés, il est possible de retracer toutes les transactions liées, et de constituer des graphiques simplifiés.

[88] http://fc14.ifca.ai/papers/fc14_submission_11.pdf

que le Bitcoin. L'évolution de leur adoption (plus ou moins large) par les utilisateurs justifiera de la pertinence de l'observation de ces flux dans la lutte contre le terrorisme et la criminalité organisée.[89]

1.9 Conclusion

Daesh n'emploie pas aujourd'hui Bitcoin pour ses donations et échanges monétaires. Cette position peut s'expliquer par l'absence de communauté utilisant Bitcoin dans la zone géographique, ou par le faible accès à Internet. Elle peut aussi s'expliquer par le fait que Daesh n'a aujourd'hui pas besoin de fonds supplémentaires pour son bon fonctionnement. Mais le cas de Daesh est un cas d'espèce présentant ses propres spécificités, et n'a pas nécessairement vocation à s'appliquer de façon générale. Force est de constater que la cryptomonnaie répond à certains critères d'anonymat et de flexibilité, et que d'autres cellules terroristes ont déjà opté, au moins ponctuellement, pour des solutions de monnaies virtuelles.

D'une part, la montée en puissance des cryptomonnaies chiffrées et intégrant le blanchiment par défaut pourrait faire changer d'avis certaines organisation terroristes. L'activité forensique sur le Darknet, et plus précisément l'analyse des flux de monnaies virtuelles constitue aujourd'hui une mine d'information considérable, et donc une opportunité majeure pour l'investigation et la compréhension des activités illicites. Mais l'évolution déjà amorcée de ces moyens de paiement vers des protocoles plus anonymes rendra certainement la tâche plus complexe.

D'autre part, la création d'une cryptomonnaie propre (à l'image du eDinar) irait dans le droit fil de la volonté de Daesh, par exemple, de disposer de sa propre monnaie, manifestation incontournable d'une souveraineté étatique efficiente. Aussi, cela ne surprendrait pas les observateurs conscients de l'appétence des sympathisants de Daesh pour les nouvelles technologies.

Mais cette transition vers la cryptomonnaie n'aurait de sens que pour certains usages bien précis. Si les donations issues du monde entier peuvent transiter par Internet, le défraiement de certaines activités ne peut se faire qu'en monnaie physique (pots de vin, achat d'armes, vente de matières premières, collecte d'impôts…). Cette part encore importante d'échanges traditionnels relègue l'usage des cryptomonnaies au rang d'outil de financement ponctuel.

[89] http://cdn.anonymousbitcoinbook.com/darkcoin/darksend-paper/