Lettre n°40 - juillet 2015 - disponible sur omc.ceis.eu

"AI technology has reached a point where the deployment of such systems is– practically if not legally feasible within years, not decades, and the stakes are high. Autonomous weapons have been described as the third revolution in warfare, after gunpowder and nuclear arms"
Extrait d'une lettre d'Elon Musk, Steve Wozniak, Demis Hassabis et Stephen Hawking écrite pour l'IJCAI, conférence internationale sur l'intelligence artificielle

Table des matières

INDUSTRIE DE LA CYBERSECURITE : QUELLES SYNERGIES PUBLIC-PRIVE ?

Le développement de la filière cybersécurité ne peut pas reposer sur le seul secteur privé, car la cyberdéfense d'un Etat exige une réponse et des capacités à la fois publiques et privées. Contrairement à une erreur souvent faite, il n'y pas d'un côté la cyberdéfense militaire et de l'autre la cybersécurité civile, mais un ensemble de capacités de cyber-protection et de cyber-défense, civiles et militaires, privées et publiques, concourant à la cyberdéfense de l'Etat[1]. Pour être efficientes, ces capacités ne peuvent pas être seulement juxtaposées. Une véritable coopération public-privé doit être mise en place. En France, 60% environ des infrastructures sensibles sont en en effet gérés par des opérateurs privés (80 % aux Etats-Unis). D'où l'émergence de législations (comme la Loi de Programmation Militaire en France), imposant aux opérateurs privés la réalisation régulière d'audits et l'adoption de mesures de sécurité.

Synergies opérationnelles

Même si elle est nécessairement fondée sur des contraintes réglementaires imposées au secteur privé, la coopération public-privé doit être aussi renforcée et entretenue par le développement de synergies entre les deux secteurs. Synergies opérationnelles, tout d'abord, afin de créer une relation de confiance entre les deux parties. Dans le contexte post-Snowden, celle-ci ne va pas de soi… les entreprises sont de plus en plus soucieuses de ne pas brouiller leur image en participant à des dispositifs que le public assimile trop rapidement à de l'espionnage. Elles craignent également de se voir imposer des mesures coûteuses et des échanges d'information à sens unique.

La création du Cyber Threat Intelligence Integration Center[2] en février 2015 par Barack Obama a ainsi soulevé quelques critiques du secteur privé américain, largement échaudé par la coopération forcée des entreprises privées avec la NSA. *« Cela doit être une mission partagée. Le Gouvernement ne peut pas faire cela tout seul. Mais le secteur privé ne peut pas le faire tout seul non plus »,* expliquait Barack Obama à Stanford quelques jours avant pour déminer le terrain. *« J'ai signé un nouvel executive order pour promouvoir les échanges d'information sur les cybermenaces, à la fois au sein du secteur privé, et entre le Gouvernement et le secteur privé. Et cela encouragera plus d'entreprises et d'industries à mettre en place des hubs permettant de partager l'information. Cela plaide pour l'adoption de standards communs, incluant la protection de la vie privée et des libertés civiles, pour que le Gouvernement puisse partager des informations avec ces hubs plus facilement. Et cela sera plus simple pour les entreprises d'accéder à l'information classifiée utile à leur protection* »[3].

[1] L'ANSSI définit la **cybersécurité** comme un *« état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles (…)».* La cyberdéfense est, quant à elle, un *« ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels ».*

[2] Cette nouvelle organisation a pour objectif de fusionner le renseignement issu des différentes agences fédérales et du secteur privé. https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center

[3] https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

Synergies industrielles

Si elle est d'abord un impératif opérationnel, la coopération public-privé doit également se traduire par la recherche de synergies industrielles et, pour ce faire, donner lieu à la mise en place d'une véritable politique industrielle. Créer des entreprises, leur faire atteindre une taille critique, est une gageure. Mais force est de constater que c'est encore plus difficile dans le domaine de la cybersécurité. Même si le marché (évalué à 70 milliards d'euros environ au niveau mondial dont 3 milliards environ en France) est bien réel et en progression de 10% par an, les investisseurs sont en effet souvent rebutés par certaines de ses caractéristiques : forte intensité en R&D, et donc en capital ; retour sur investissement moins rapide que pour d'autres segments du numérique ; rôle support ou facilitateur - et donc souvent perçu comme annexe - de la sécurité par rapport à la fonctionnalité principale ; croissance largement liée à des « drivers » réglementaires et à la peur des attaques informatiques, non à des anticipations positives.

Le développement d'une filière industrielle en cybersécurité, qui répond à la fois à une nécessité stratégique et à une opportunité économique, ne peut donc résulter uniquement des forces du marché. Il doit être accompagné, soutenu et « accéléré ». C'est la raison d'être des clusters, incubateurs et accélérateurs et qui se sont multipliés depuis quelques années dans le domaine.

Quelques définitions

Cluster : « un cluster est "un groupe d'entreprises et d'institutions partageant un même domaine de compétences, proches géographiquement, reliées entre elles et complémentaires" (Porter, 1999). Le "cluster" est donc un regroupement d'entreprises et d'institutions faisant partie d'un même secteur d'activité (même domaine de compétences) et qui sont ancrées dans un territoire ou localisées géographiquement. Ce regroupement permet aux acteurs d'un cluster de bénéficier d'avantages compétitifs grâce notamment aux "externalités" qu'elles suscitent (définition de la DATAR). »[4]

Incubateur : « les incubateurs sont des espaces regroupant des entreprises nouvellement créées. Leur objectif est d'améliorer le taux de croissance et de survie de ces entreprises en leur offrant un bâtiment modulaire avec des services partagés (informatique, etc.) et un appui managérial. Le temps moyen d'incubation est de 2 ans. Les incubateurs peuvent prendre des participations dans les entreprises qu'ils accompagnent dans leurs premières années pour les revendre ensuite. »[5]

Accélérateur : « les accélérateurs s'adressent à des jeunes entreprises en phase de démarrage ou ayant déjà une activité et opérant très souvent dans le high-tech. Ils se focalisent surtout sur l'offre de formations techniques et un espace Web gratuit, contrairement aux incubateurs qui offrent des espaces locatifs. Souvent dirigés par des spécialistes du capital risque, les accélérateurs se rémunèrent en prenant des participations dans les startups qu'ils préparent à leurs premiers rounds de financement auprès de capitaux-risqueurs. »[6]

[4] http://www.univ-nantes.fr/82467798/2/fiche___pagelibre/&RH=1182582642425

[5] http://executivebusinessaccelerator.com/quelle-difference-y-a-t-il-entre-un-incubateur-un-accelerateur-et-lexectutive-business-accelerator/

[6] Ibid

Quatre objectifs complémentaires

Tous ces projets complémentaires partagent, à des degrés divers, quatre objectifs :

- Le soutien à la R&D. C'est par exemple l'objectif des programmes RAPID de la Direction Générale de l'Armement, du Programme des Investissements d'Avenir piloté par le Commissariat général à l'investissement ou du programme Horizon 2020 de la Commission européenne. Toute la difficulté consiste ensuite à transformer les prototypes en produits industriels et à ne pas « étouffer » les startups par des subventions uniquement orientés vers de la recherche très amont.

- L'accès au marché. C'est l'un des leviers les plus compliqués à mettre en œuvre. Outre les opérations traditionnelles de promotion (participation à des salons, showrooms…), il s'agit surtout de favoriser l'achat par les administrations et par les grandes entreprises de solutions produites par les startups et PME. Ces grandes structures rechignent en effet trop souvent à contracter avec des petites structures, contraignant celles-ci à nouer des partenariats, pas toujours très bénéfiques pour elles, avec des intégrateurs. Ce fut l'une des raisons de la création de l'association Hexatrust[7], réunissant une vingtaine de PME et ETI françaises du domaine de la cybersécurité et de la confiance numérique : mutualiser les moyens pour être plus fort. L'accélération « business » doit donc être une priorité. C'est par exemple le sens du CyberLab™ lancé par CEIS en 2014.

- L'accès au financement. Si l'amorçage est en général bien soutenu en France, le développement se révèle lui nettement plus difficile. Les fonds considèrent en effet que les perspectives de sortie sont limitées, notamment en raison de l'absence d'éditeurs susceptibles de racheter à termes les entreprises dans lesquels ils investissent. Certains fonds commencent cependant à observer avec intérêt le secteur. Calao Finance est ainsi en train de développer un fonds dédié à la cybersécurité, lequel devrait être opérationnel en fin d'année. On reste cependant loin de la situation américaine où, selon le *Financial Times,* qui cite le cabinet d'études PrivCo, les fonds de capital-risque américains ont investi plus de 1,2 milliards de dollars dans les startups américaines spécialisées dans la cybersécurité au premier trimestre 2015, soit une augmentation de 122% par rapport à 2014[8].

- Le développement d'une main d'œuvre spécialisée, grâce à des cursus diversifiés en termes de niveaux et de disciplines et à la mise en place de mesures permettant de favoriser les échanges entre secteur public et secteur privé[9].

Panorama des clusters, incubateurs et accélérateurs spécialisés

Ce panorama, non exhaustif, souligne le rôle clé joué par ces structures dans le développement de la filière cybersécurité et la structuration du marché. Ces organisations sont pour la plupart financés par des fonds publics et privés.

➡ Etats-Unis

Les Etats-Unis comptent de nombreuses organisations ou programmes spécialisés :

- L'université du Maryland a créé le Cyber Incubator BWtech[10], situé non loin du siège de la NSA à Fort Meade. Cet incubateur s'appuie sur

[7] http://www.hexatrust.com/

[8] http://frenchweb.fr/aux-etats-unis-les-investissements-dans-la-cybersecurite-ont-plus-que-double-sur-un-an/191522

[9] Voir à ce propos la note stratégique réalisée par CEIS à la suite d'une Etude de Prospective Stratégique réalisée pour la DGRIS (http://www.ceis.eu/fr/actu/note-strategique-comment-developper-la-main-d-oeuvre-specialisee-en-cybersecurite)

[10] http://www.bwtechumbc.com//

deux programmes : le CYNC, qui résulte d'un partenariat entre l'incubateur et Northrop Grumman, explore 5 axes : cyber, data sciences, big data, secure mobility, cyber physical systems ; CyberHive, qui est un espace de co-working et qui propose un certain nombre de moyens aux startups du secteur. A noter que ce CyberHive a depuis essaimé à San Diego[11] ;

- Opérationnel depuis 2013, Match37 est un accélérateur public-privé hébergé au Virginia Tech Research Center[12]. Il propose un environnement de simulation accessible à distance et a déjà incubé plusieurs jeunes sociétés : Cyberpath (environnement de simulation), Key Security (analyse forensique), Pierce Global Threat Intelligence (détection), CyberLingua (analyse de trafic et détection de 0 day), Sikernes (ERP dédié à la cybersécurité).

- Le Air Force Research Laboratory a monté un programme pilote destiné à commercialiser les technologies du DoD auprès d'acteurs privés[13]. Les entreprises sélectionnées peuvent ensuite participer au programme New York Furnace Technology Transfer Accelator. L'objectif est ainsi de lancer entre 5 et 10 startups, dont certaines sur la cybersécurité, d'ici 2015 en partenariat avec l'Université de l'Arizona.

- La CIA a créé en 1999 In-Q-Tel[14]. Ce fond américain de capital-investissement à but non lucratif prend des participations stratégiques dans des entreprises technologiques de pointe, notamment des startups liées à la collecte, l'analyse et au traitement de l'information, en lien avec le renseignement. Les participations permettent souvent d'avoir un siège au conseil d'administration et donc de connaître et de suivre les évolutions technologiques des entreprises. Sa politique d'investissement massif et sans recherche de profits en fait un partenaire privilégié pour les entrepreneurs des domaines de pointe : Gemplus/Gemalto (carte à puce), Recorded Future (cyber threat intelligence), Palantir Technologies (visualisation de données).

On note également l'existence de l'association SINET[15], un « super connector » dont l'objectif est de faciliter la collaboration entre secteur public et privé dans le domaine de la cybersécurité et qui est notamment soutenu par le DHS.

➡ OTAN

La NATO Communications and Information Agency (NCIA) a lancé en février 2015 un incubateur pilote en cybersécurité. Trois thématiques ont été sélectionnées (« big data analysis for cybersecurity, Cyber Situational Awareness, Mobile Security ») et 50 sociétés et organisations[16] ont déjà rejoint le programme, dont Thales sur la partie « Cyber Situational Awareness ». Les premiers résultats du pilote seront présentés lors d'un symposium qui se tiendra les 15 et 17 septembre à Mons[17].

➡ Israël

Israël, souvent baptisée la nation « startup », compte au moins deux incubateurs de renom :

- Le cyber Labs, lancé début 2014, par Jerusalem Venture Partners en partenariat avec l'université Ben Gourion dans le cadre du Chief

[11] http://www.sandiegouniontribune.com/news/2013/feb/15/CyberHive-San-Diego-focused-on-cyber-security/

[12] https://ctovision.com/2013/09/mach37-americas-premier-market-centric-cybersecurity-accelerator/

[13] http://defensesystems.com/articles/2014/06/18/afrl-spawar-commercialize-tech.aspx?m=2
http://www.wpafb.af.mil/news/story.asp?id=123414764

[14] https://www.iqt.org/

[15] http://www.security-innovation.org/

[16] https://www.ncia.nato.int/NewsRoom/Pages/150706-CyberSecuritySL-innovation-pilot.aspx

[17] https://www.ncia.nato.int/Events/Pages/150515-NIAS2015.aspx

Scientist Incubator Program. Situé non loin de la puissante Telecommunications Division des forces de défenses israéliennes (IDF), cet incubateur s'est distingué en investissant dans CyActive, une startup spécialisé dans l'analyse prédictive des menaces informatiques, société rachetée par Paypal en mars 2015 ;

- Team8 Ventures, fondé début 2015 par Nadav Zafrir, l'ancien patron de l'unité 8200 avec plusieurs anciens de cette même unité. Financé par Eric Schmidt, le président de Google, Bessemer Venture Partners, Marker LLC avec la participation de Cisco et d'Alcatel-Lucent, cette structure a adopté un modèle original : elle fonctionne comme une société indépendante avec ses propres salariés et essaime ensuite en fonction des projets qui débouchent.

➡ Grande-Bretagne

Co-fondé par Alex van Samoren d'Amadeus Capital Partners, également fondateur de nCipher, Jonathan Luff et Grass Cassy, co-fondateurs du cabinet de conseil Epsilon Advisory Partners, CyLon[18] a été fondé en janvier 2015 à Londres. Il incube à ce jour six sociétés[19] : Aimbrain (environnement biométrique pour mobile), Cyber Defence Technologies (solution BYOD), Cyberlytic (analyse de risque), Intruder (investigation numérique), Mentat Innobations (analyse big data) et Ruuta (routeur wifi « social »). Cette organisation à but non lucratif a été inaugurée en présence de Sir Iaian Lobban, ancien directeur du GCHQ.

Le GCHQ soutiendrait par ailleurs la création prochaine d'un incubateur défense et sécurité à Bristol[20]. Il pilote également un Centre d'innovation dans le Gloucestershire ouvert au secteur privé « habilité » et envisage d'étendre cette initiative à l'ensemble des startups et PME. Le GCHQ organise à ce sujet un UK Cyber Security Industry Summit (IA15) qui aura lieu en décembre 2015 à Londres.

➡ Canada

Le pays a créé un premier incubateur dédié en 2014. Géré par Venus Cybersecurity[21], une organisation à but non lucratif, il héberge notamment Strike, un éditeur, et WAW Technologies, qui produit des sondes de détection.

➡ Singapour

Le pays compte près d'une trentaine d'incubateurs fonctionnant dans le cadre du Technology Incubation Sheme mis en place en 2008 par le National Framework for Innovation and Enterprise Programme. Il permet à la National Research Foundation de co-investir jusqu'à hauteur de 85 % dans une startup basée à Singapour, le reste étant apporté par l'incubateur.

➡ France

La France aujourd'hui compte deux clusters spécialisés qui offrent diverses prestations de financement de projet et d'accélération :

- Le pôle d'excellence Cyberdéfense (PEC). Ce cluster de portée nationale possède trois dimensions : la recherche ; la formation initiale, continue et l'enseignement supérieur ; le développement du tissu industriel ;

---

[18] https://cylonlab.com/

[19] http://techcrunch.com/2015/04/16/london-security-incubator-cylon-selects-first-cohort/

[20] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

[21] http://www.venuscyber.com

LA CYBERDEFENSE MILITAIRE AU SEIN DE LA CYBERDEFENSE NATIONALE

En France, le monde militaire et le monde civil font l'objet d'une nette séparation au sein du cyberespace. Le ministère de la Défense s'occupe uniquement de son périmètre, en conduisant la défense des systèmes d'information du ministère et des armées et en soutenant les opérations militaires grâce à des capacités informatiques défensives et offensives. C'est donc à l'ANSSI d'être en charge avec le COSSI (Centre opérationnel de la sécurité des systèmes d'information) des opérateurs d'importances vitales (OIV), des autres ministères et de la stratégie nationale de cybersécurité. Ce modèle n'est pas forcément celui adopté par d'autres pays comme les Etats-Unis ou le Brésil.

Le cas français

Il est d'abord nécessaire d'observer les différents moments où la cyberdéfense militaire intègre la cyberdéfense nationale. Prenons l'exemple de la France.

Tout d'abord, au niveau opérationnel, le ministère de la Défense et l'ANSSI travaillent main dans la main. Par exemple, la co-localisation du centre de cyberdéfense de l'ANSSI avec le centre d'analyse de lutte informatique défensive (CALID) du ministère de la Défense permet d'assurer une coordination étroite entre les deux centres. La cinquantaine d'agents de l'ANSSI peuvent travailler ainsi avec la soixantaine de personnes du CALID, qui sont eux placés sous l'autorité de l'officiel général cyberdéfense du ministère de la Défense. De plus, l'implication du ministère de la Défense au sein de l'écosystème national est aussi soulignée par la mise en place d'une véritable stratégie de sensibilisation, avec l'aide principale de la réserve citoyenne cyberdéfense (RCC). Composée de 150 membres, répartis en 7 groupes de travail, la RCC est présentée par le ministère de la Défense comme « le réseau de réserve citoyenne cyberdéfense qui vise à faire de la cyberdéfense une priorité nationale à travers des actions de sensibilisation.[22] »

De même, la DGA a depuis de nombreuses années contribué au développement technologique français en finançant des projets innovants à double usage civil et militaire. Ainsi, le ministre de la Défense Jean-Yves Le Drian a évoqué au FIC 2014 à Lille : « *Nous allons tripler le volume des études consacrées à la cyberdéfense, et par ailleurs nous allons poursuivre la montée en puissance de notre dispositif Rapid »*[23] Le dispostif Rapid[24] (« régime d'appui aux PME pour l'innovation duale »), lancé conjointement par les ministères de l'économie et de la défense, vise à soutenir des projets de recherche industrielle ou de développement expérimental à fort potentiel technologique, présentant des applications militaires mais aussi des retombées pour les marchés civils. Ainsi, la cyberdéfense militaire contribue au développement d'un secteur où la technologie

[22] http://www.defense.gouv.fr/reserves/monde-de-la-reserve/cyberdefense/le-reseau-de-la-reserve-citoyenne-cyberdefense

[23] http://www.01net.com/editorial/612470/le-gouvernement-debloque-un-milliard-deuros-pour-la-cyberdefense/

[24] http://www.service-public.fr/professionnels-entreprises/actualites/00521.html

doit être constamment améliorée et de nouvelles solutions développées.

Enfin, le ministère de la Défense réfléchit sur son implication lors d'une attaque cybernétique. En effet, au titre des grandes fonctions stratégiques de la Défense, comme la protection du territoire et des populations dans le cadre de la posture permanente de sécurité (PPS), le ministère de la Défense pourrait avoir une légitimité à agir dans le cyberespace national, lors d'une crise majeure par exemple. La Défense peut ainsi amener un renfort aux forces de sécurité intérieure et de sécurité civile en engageant des forces terrestres, navales et aériennes, qui seraient « complétées par le dispositif de cyberdéfense », comme précisé dans le livre blanc sur la défense et la sécurité nationale de 2013[25].

Ainsi, nous pouvons observer que dans le cas français, la cyberdéfense militaire contribue au secteur de la cyberdéfense à l'aide de financement, de sensibilisation, et de collaboration étatique. Actuellement, le ministère de la Défense n'intervient pas directement au sein de la cyberdéfense nationale (sauf peut-être en cas de crise majeure), contrairement à d'autres pays, comme les Etats-Unis par exemple.

Le ministère de la Défense, acteur de la cyberdéfense nationale.

En effet, les Etats-Unis ont une stratégie différente. Le monde militaire est fortement présent au sein du cyberespace du pays où il y joue un rôle important. Le renseignement électronique et la cybersécurité y sont co-localisés au sein d'une même entité, la NSA.

La National Security Agency (NSA) est un organisme gouvernemental sous le commandement du département de la Défense américaine (DoD). La NSA assure les activités de renseignement SIGINT et la sécurité de l'information des systèmes de sécurité nationale. L'Information Assurance Directorate (IAD) assure, au sein de la NSA, l'expertise sur les questions de cryptographie et de protection des systèmes d'information et compte environ 3 000 agents. Cette direction, qui par ailleurs contribue à traiter les incidents opérationnels, est l'homologue de l'ANSSI. De plus, le département de la Défense américaine a publié sa cyberstratégie en avril 2015. Dans ce dernier, elle annonce que ses trois missions principales sont :

- *Defend DoD networks, systems, and information*

- *Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence*

- *Provide cyber support to military operational and contingency plans*

Par ses missions, nous comprenons que l'un des objectifs principaux du DoD est de défendre le territoire américain et les intérêts nationaux des États-Unis contre les cyberattaques aux fortes conséquences. Par ailleurs, dans cette doctrine, le département de la Défense américaine décrit son niveau d'implication au sein de la cyberdéfense nationale *"In concert with other agencies, the United States Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. In a manner consistent with U.S. and international law, the Department of Defense seeks to deter attacks and defend the United States against any adversary that seeks to harm U.S. national interests during times of peace, crisis, or conflict. To this end the Defense Department has*

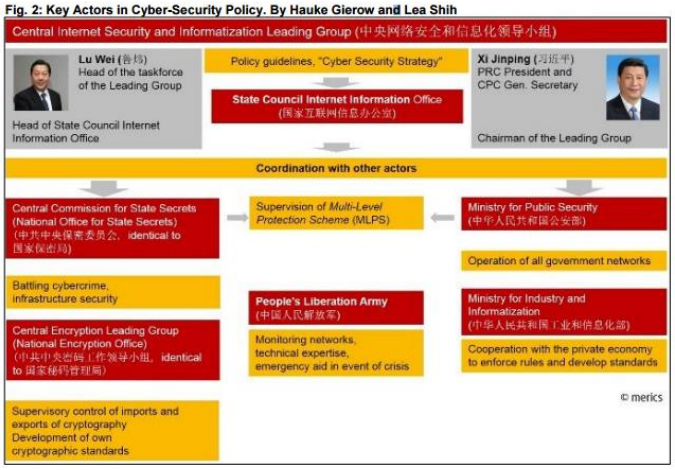
[25] http://fr.calameo.com/read/000331627d6f04ea4fe0e - page 91

developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic, informational, military, economic, financial, and law enforcement tools." Le DoD précise donc que son rôle est de défendre les intérêts nationaux, y compris diplomatiques, informationnels, militaires, économiques, financiers.

Nous avons d'ailleurs pu observer l'implication du DoD lors de l'attaque de Sony Pictures qui s'est déroulée en novembre 2014[26]. Bien que cette société soit privée, le département de la Défense a joué un rôle public dans la résolution de cette attaque, venant ainsi soutenir le FBI. Toutefois, leurs discours différaient au début de l'affaire, ce qui a engendré la création du CTIIC : le Cyber Threat Intelligence Integration Center[27]. Ce centre d'intégration du renseignement sur les cyber-menaces n'aura pas pour rôle de rechercher des renseignements sur les attaques informatiques mais d'améliorer la cybersécurité en centralisant ceux récoltés par de multiples biais (agences gouvernementales et sociétés privés) et ainsi d'émettre une communication unique des différentes agences gouvernementales (FBI, DoD, NSA, CIA, etc.). De plus, comme en France, le département de la Défense américaine montre une volonté d'avoir une forte présence au sein du cyberespace national en termes de soutien. Un vaste programme est présenté dans la nouvelle stratégie du DoD. Celui-ci engendrera pour le ministère des investissements sur le long terme importants et des efforts en R&D mobilisant défense, monde académique et industries. De même, l'objectif est d'encourager la collaboration entre le DoD et les industriels. Ainsi en mai 2015 suite à la publication de la cyberstratégie du DoD, le secrétaire à la Défense Ash Carter a parcouru pendant 2 jours la Sillicon Valley afin de « renouveler les liens de confiance et de reconstruire le pont entre le Pentagone et la Silicon Valley. ».

Autre exemple : on peut observer en Chine qu'une partie de la cyberdéfense nationale est sous l'égide de l'Armée Populaire de Libération (APL). Cette dernière a la responsabilité de surveiller les réseaux, d'avoir une expertise technique et de fournir de l'aide lors des crises. Ci-dessous, un organigramme des responsabilités sur le domaine du cyberespace au sein du gouvernement chinois.

Fig. 2: Key Actors in Cyber-Security Policy. By Hauke Gierow and Lea Shih



Source : http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf

Au sein du document stratégique chinois « China's Military Strategy »[28] publié le 26 mai 2015 par son ministère de la Défense, il est écrit que «Le cyberespace est devenu un nouveau pilier du développement économique et social, ainsi qu'un

[26] http://www.govtech.com/security/Sony-Pictures-Hack-Redefines-Rules-of-Online-Warfare.html

[27] https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center

[28] http://news.usni.org/2015/05/26/document-chinas-military-strategy

nouveau domaine de la sécurité nationale. Comme la concurrence internationale dans le cyberespace devient de plus en plus compétitive, de nombreux pays développent leurs forces militaires cyber. Etant l'une des principales victimes des attaques de pirates, la Chine est confrontée à des menaces graves sur son infrastructure informatique. Comme le cyberespace a un poids plus important dans la sécurité militaire, la Chine va accélérer le développement d'une force cyber et renforcer ces capacités dans le cyberespace de prise de connaissance de la situation, de cyberdéfense, de soutien aux efforts du pays et la participation à la coopération internationale de manière à endiguer les crises majeures cyber, assurer la sécurité des réseaux et de l'information nationaux, et de maintenir la sécurité nationale et la stabilité sociale. »

En Chine, nous pouvons observer une très grande porosité entre la sphère politique et la sphère des entreprises d'Etat qui est majoritairement représentée par l'Etat lui-même et des agences gouvernementales chinoises placées sous la tutelle administrative de la Commission d'administration et de supervision des actifs publics du Conseil des affaires de l'Etat (SASAC). Le choix des responsables des entreprises d'Etat des secteurs stratégiques et prioritaires demeure intimement contrôlé par le gouvernement chinois. La classification entre les entreprises d'Etats des secteurs dits « stratégiques » et les entreprises d'Etat des secteurs dits « piliers » pour l'économie chinoise par la SASAC remonte à la publication en 2006 d'une directive intitulée « Avis concernant la promotion de l'ajustement des actifs de l'Etat et la réorganisation des entreprises d'Etat »[29]. Il en résulte que le secteur des télécommunications fait partie des secteurs dits « stratégiques » alors que le secteur des technologies de l'information fait quant à lui partie des secteurs dits « piliers » de l'économie chinoise.

L'armée, au centre de la cyberdéfense nationale.

D'autres pays, comme le Brésil, ont une stratégie plus « radicale ». Ainsi, en 2011, suite au *Strategic Cyber Defense Project*[30], Brasilia a donné la plupart des responsabilités de la cybersécurité à l'armée. Il a été fourni à l'armée brésilienne un dispositif afin de pouvoir surveiller les affaires civiles : le CDCiber[31]. Opérationnel depuis la fin 2011, le CDCiber (Centro de Defesa Cibernética) est une structure militaire interarmées chargée par le gouvernement brésilien de coordonner les actions de cyberdéfense. Son objectif principal est d'assurer la protection des réseaux militaires et gouvernementaux contre les attaques internes et externes. De plus, il a aussi pour objectif de protéger l'intégrité de l'infrastructure nationale de l'informatique. Pour contrecarrer les attaques informatiques, l'armée utilise aussi bien les compétences de son personnel que celles de civils. Civils, qui par ailleurs peuvent proposer des formations en cybersécurité sur la façon de détecter et de mettre fin à ces agressions par exemple. L'année 2015 revêt une importance particulière pour le secteur de la cyberdéfense au Brésil. Neuf sous-projets du *Strategic Cyber Defense Project* se concentrent principalement sur les ressources humaines de la formation ainsi que sur la recherche et le développement d'outils de défense et de sécurité en sécurité informatique. Des études et des discussions sont

[29] http://www.sasac.gov.cn/n1180/n1566/n258252/n258644/11663621.html

[30] http://seminde.com/wp-content/uploads/arquivos-2014/painel6/carvalho.ppt

[31] http://www.umass.edu/digitalcenter/research/working_papers/13_002_Canabarro-Borne_BrazilandFogofCyberWar.pdf

en cours au sein du ministère de la Défense brésilienne pour la création de la *National Cyber Defense School* et le *Cyber Defense Command*. Le ministère de la Défense stipule la création de ces organisations dans un décret d'octobre 2014 (décret réglementaire 2777 / MD[32]), dans le cadre d'une série de mesures visant à renforcer la politique de cyberdéfense du pays. L'initiative vient compléter les efforts déployés dans ce domaine par le biais de projets stratégiques en cyberdéfense de l'armée. La *National Cyber Defense School* fonctionnera comme un centre de recherche et de développement de la cyberdéfense nationale et inclura la participation aussi bien des institutions civiles et militaires que des professionnels. Le *Cyber Defense Command* devrait superviser, coordonner et fournir l'orientation technique et réglementaire pour les activités du système de cyberdéfense brésilien. Le CDCiber se concentrera uniquement sur les opérations.

Nous observons donc un véritable dégradé de situations sur l'implication des différents ministères de la Défense sur le sujet du cyberespace national. L'exemple français où la cyberdéfense militaire participe à la cyberdéfense nationale par son implication dans l'écosystème à l'aide de financements, de collaborations ou encore d'actions de sensibilisation, voir l'intervention en cas d'attaques mettant directement en cause la sécurité de la Nation. L'exemple américain et chinois où le ministère de la Défense agit sur une partie du cyberespace national en surveillant les réseaux nationaux dans le but de défendre le territoire et les intérêts des pays contre des attaques informatiques. Enfin, l'exemple brésilien où la cyberdéfense nationale est conduite principalement par le ministère de la Défense. Bien que la cybercriminalité soit le premier crime économique dans le pays (contrairement au reste du monde, où la cybercriminalité est classé quatrième.)[33], l'Etat brésilien a fait le choix de miser majoritairement sur un rôle militaire dans le cyberespace, négligeant peut-être ainsi l'intérêt du rôle du ministère de l'Intérieur. Il sera intéressant d'observer les mutations et conséquences dans les prochaines années de ces différents schémas pour l'évolution nationale de la cyberdéfense.

[32] http://pesquisa.in.gov.br/imprensa/servlet/INPDFViewer?jornal=1&pagina=7&data=28/10/2014&captchafield=firistAccess

[33] http://www.darkreading.com/vulnerabilities---threats/the-cybercrime-carnival-in-brazil-loose-cyberlaws-make-for-loose-cybercriminals/a/d-id/1320441

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** 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 **DGRIS** a confié à **CEIS** la réalisation de 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.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com