Observatoire du Monde Cybernétique

Lettre n°25 – Janvier 2014

Cette note est disponible sur le portail OMC. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

[FIC2014] Retour sur le Forum international de la Cybersécurité 2014 à Lille

L'édition 2014 du Forum International de la Cybersécurité (FIC) s'est déroulée à Lille le 21 et 22 janvier. Organisé par la Gendarmerie Nationale, Euratechnologies et la Compagnie Européenne d'Intelligence Stratégique (CEIS), il a accueilli en deux jours plus de 3400 participants, parmi lesquels les ministres français de l'Intérieur, de la Défense et le Secrétaire Générale à la Défense et la Sécurité Nationale (SGDSN). En ouverture du Forum, Manuel Valls a annoncé un renforcement de la lutte contre la cybercriminalité qui mettra l'accent sur la prévention, la sensibilisation, mais également sur une connaissance renforcée des usages et des menaces potentielles. Le ministre de la Défense a quant à lui annoncé son "pacte cyber" qui devrait permettre la multiplication par six des effectifs du Centre d'Analyse en Lutte Informatique Défensive (CALID), et le doublement de ceux de la Direction Générale de l'Armement spécialisée en Maîtrise de l'Information (DGA MI). L'application des mesures de la Loi de Programmation Militaire (LPM) adoptée en décembre 2013 a également été au cœur des discussions. L'article 13 de la loi, devenu article 20, sur l'accès administratif aux données personnelles a également fait l'objet de débat entre partisans français de la protection de la vie privée sur Internet et instances régaliennes.

Le Forum a été l'occasion de débattre sur lors nombreuses conférences et ateliers sur des thèmes juridiques, économiques, de sécurité, liés au cyber. Il a été plus international que les éditions précédentes, avec des ateliers consacrés aux stratégies cyber nationales et européennes. A titre d'exemple, l'ancien chef d'état-major du US Cyber Command américain, David Senty, a débattu avec des intervenants chinois, russes et français sur les stratégies respectives des pays. Cet aspect international devrait être encore renforcé pour les éditions à venir.

Le Forum permettait également aux entreprises spécialisées en cybersécurité et numérique d'exposer leurs solutions aux visiteurs. Si les grandes entreprises françaises du secteur étaient présentes, un espace innovation permettait également aux PME d'exposer leurs offres. Un challenge de hacking ainsi que des démonstrations techniques ont eu lieu pendant les deux jours.

[Silicon] Piratage du câble sous-marin : le pétard mouillé qui met le feu à la presse française

Der Spiegel a révélé que la National Security Agency (NSA) américaine avait réussi à pénétrer le site d'administration et de gestion du câble sous-marin SEA-ME-WE4 qui relie la France (depuis Marseille) à Singapour. La construction de ce câble a démarré en 2004, sur décision et financement d'un consortium de 16 entreprises dont l'opérateur télécom Orange, qui possède un accès au site pénétré par les "forces spéciales de la NSA", une équipe appelée Tailored Access Operations (TAO). Cette révélation a connu un fort écho dans la presse française du fait de la crainte d'un piratage direct de Orange ou d'interception des données transitant dans le câble. Or, l'opération s'est révélée être une simple pénétration de site internet auquel Orange a accès, et qui contient des informations sur la structure, le tracé et l'état du câble.

[L'Express] Le Drian : un plan pour "préparer la France à la guerre cybernétique"

Lors du Forum International de la Cybersécurité (FIC) 2014, le ministre de la Défense a annoncé un "plan de défense cyber" pour préparer la France à la "guerre cybernétique". Celui-ci nécessitera l'engagement de 1 milliard d'euros d'ici 2019. Ces investissements conséquents ont pour but de "changer d'échelle" et de devenir en mesure de lutter contre le nombre croissant de cyberattaques. Il a indiqué que les attaques significatives répertoriées en 2013 étaient au nombre de 780, contre seulement 195 en 2011. Les effectifs du Centre d'Analyse et de Lutte Informatique Défensive (CALID) devraient être multipliés par six (passant de 20 à 120 personnes) tandis que ceux de la DGA Maîtrise de l'Information (DGA MI) située à Bruz devraient passer de 250 à 450. Il a insisté sur la nécessité d'apporter de "nouvelles capacités défensives et

offensives, appuyées par un renseignement d'intérêt cyber".

[Le Parisien] Châtillon : vol d'ordinateurs contenant des données sensibles chez Siemens

Jeudi 9 janvier, une trentaine d'ordinateurs contenant des données sensibles ont été dérobés sur le site de la société Siemens à Châtillon. Les cambrioleurs sont parvenus à pénétrer le site sans effraction pour s'emparer du matériel informatique.

[Data Security Breach] J.O. de Sotchi, les jeux olympiques de l'espionnage ?

Selon des documents récupérés par des journalistes russes, le Service fédéral de sécurité (FSB) « prévoit de faire en sorte qu'aucune communication, de la part des concurrents comme des spectateurs, n'échappe à la surveillance ». Le FSB a récemment opéré une montée en puissance de ses capacités cyber avec la création du Cyber Command russe en son sein. La surveillance de masse pour les jeux olympiques devrait faire appel à ces capacités, comme ce fut le cas à moindre échelle pendant le G20 et l'affaire des clés USB et des chargeurs de téléphones infectés par des logiciels malveillants.

[HackRead] Le Parlement Européen invite Edward Snowden à témoigner contre la surveillance de la NSA

Le Comité Libertés civiles, justice et affaires intérieures a voté à 36 contre deux et une abstention en faveur du témoignage d'Edward Snowden devant le Parlement européen. Les révélations de la NSA avaient soulevé de nombreuses protestations au sein des institutions européennes, ainsi que des demandes de suspension des négociations sur l'accord de libre échange entre avec les Etats-Unis. Alors que les députés souhaiteraient pourvoir avoir un échange interactif, le témoignage ne devrait pas se faire en temps réel, car les Etats-Unis seraient capables de localiser Edward Snowden le cas échéant. A l'heure actuelle, Edward Snowden n'a pas encore accepté l'invitation et aucune date n'a été arrêtée pour l'interview.

[Le Monde] Le Kremlin va surveiller ses détracteurs sur Internet

Le service en charge de la sécurité du Kremlin, le FSO, va renforcer la surveillance des blogueurs russes en utilisant un système recueillant des données de manière quotidienne sur ses cibles. L'objectif à travers ce programme révélé par le journal Izvestia est de créer des bases de données sur les blogueurs ayant une opinion négative du pouvoir en place. Ce programme existait déjà au sein de l'administration, mais sera dorénavant confié à des "informaticiens professionnels" du fait de l'ampleur qu'il prend à l'occasion des JO de Sotchi.

[Silicon] Clean Pipe : le bouclier anti NSA de Deutsche Telekom, sera finalisé pour 2016

L'opérateur télécom allemand a initié les tests de son service baptisé "Clean Pipe" sur quelques PME et TPE. Ce service a pour objectif d'être un "bouclier numérique" assurant un périmètre de sécurité aux données qui transitent sur le réseau de Deutsche Telekom en les conservant sur le territoire national.

Développé en réaction aux écoutes de la NSA, "Clean Pipe" est supposé être exempt de toute "backdoor" ou vulnérabilité exploitées par les services américains.

[VOA] Moscou allonge le droit d'asile d'Edward Snowden

Lors d'une réunion sur "le futur de la puissance américaine" au Forum Economique Mondial de Davos, le chef du comité des affaires étrangères de la Douma, Alexey Pushkov, a déclaré que Moscou n'avait aucune intention d'expulser Edward Snowden. Ce dernier ne "sera pas renvoyé de Russie" selon ses termes. L'allongement du droit d'asile initial d'une durée d'un an permettrait à Edward Snowden un jugement "sans clémence" aux Etats-Unis.

[Arstechnica] Des hackers auraient compromis des communications chiffrées sur TOR

Des scientifiques ont découvert plus de 20 ordinateurs utilisés pour saboter TOR, en surveillant et modifiant les données passant du serveur à l'utilisateur final.

S'il n'a pas été possible de découvrir qui avait intentionnellement mal configuré les serveurs, 19 des 22 serveurs découverts étaient gérés par une seule personne ou un seul groupe en Russie.

[Le Monde] Le compte Twitter de Skype piraté par l'Armée électronique syrienne

La Syrian Electronic Army, un groupe de hackers favorable à Bachar Al-Assad, a piraté le 1er janvier le compte Twitter de Skype et publié le message suivant: « n'utilisez pas le service de mails de Microsoft [Hotmail, Outlook], ils surveillent vos comptes et vendent les informations aux gouvernements ».

Si la SEA a effectué plusieurs piratages de comptes officiels américains en 2013, elle fait ici référence à l'affaire Snowden et la révélation de documents montrant la coopération de Microsoft avec la NSA, notamment dans le cadre du programme PRISM de collecte de données.

[Igen] Apple récuse toute collaboration avec la NSA

Suite aux révélations montrant que la National Security Agency (NSA) américaine disposait de "porte dérobées" lui permettant d'extraire des données à partir de tous les iPhones, Apple a publié un démenti. L'entreprise récuse toute collaboration avec la NSA et n'aurait jamais entendu parler de DropoutJeep, le logiciel qui permettrait de collecter les données voulues sur les iPhones en se servant d'une "porte dérobée".

Des documents, révélés par Der Spiegel, montrant la méthode de la NSA datent de 2008, peu après le lancement du premier iPhone.

[US Naval Institute] Time for a U.S. Cyber Force - Le temps d'une Force Cyber est venu

L'amiral James Stavridis et David Weinstein plaident pour la mise en place de forces cyber sur le même modèle que celui des Forces Spéciales américaines et leur commandement (SOCOM). Ce CYBERCOM permettrait de gagner en efficacité et cohérence par rapport au modèle actuel, dans lequel chaque armée dispose de sa propre version d'un cyber command.

[Infosecurity] La Californie cherche à mettre en place un "kill switch" sur les smartphones

Le sénateur Mark Leno et le procureur général de San Francisco Georges Gascon souhaitent faire de la Californie le premier Etat à disposer d'un "kill switch", une solution qui permettrait aux propriétaires d'un smartphones de le désactiver en cas de vol. Face à l'augmentation drastique des vols de smartphones, qui constituent plus de 50% de tous les actes de vol effectués en 2013 en Californie, l'installation d'un tel dispositif se révélerait efficace. Certains s'inquiètent cependant de la capacité de l'Etat à également utiliser ce "kill switch" en cas d'aboutissement du projet.

[Washington Post] Obama signe la nomination de Rogers à la direction de la NSA

Le Président américain Barack Obama a signé la nomination du vice-amiral Rogers à la tête de la NSA. De manière habituelle mais révélatrice de l'importance du poste, le Président aurait lui-même mené l'entretien précédant la nomination. Celle-ci devrait être effective au plus tard en mars.

Le vice-amiral Rogers était depuis octobre 2013 favori à la succession du général Alexander aujourd'hui encore directeur de la NSA et du US Cyber Command. Fort de son expérience à la tête du Cyber Command de la Navy, le vice-amiral aurait été désigné comme "seul suffisamment qualifié" pour un poste extrêmement médiatisé et critiqué en 2013.

[HackRead] Des ordinateurs du ministère de la Défense israélien piratés par des hackers palestiniens

Selon Aviv Raff, directeur de la technologie de Seculert, des hackers auraient réussi à pénétrer jusqu'à 15 ordinateurs du ministère de la Défense israélien.

L'attaque aurait eu lieu par le biais de faux e-mails, ressemblant à ceux du Shin Bet, et contenant une pièce jointe infectée. Elle aurait été attribuée à des hackers palestiniens du fait de sa ressemblance avec une attaque ayant eu lieu un an auparavant et provenant de servers contrôlés par le Hamas dans la Bande de Gaza.

Le logiciel malveillant ayant permis la première infection serait "Xtreme RAT". L'attaque a eu lieu juste après l'intervention du Premier ministre israélien Benjamin Netanyahu au Forum Economique Mondial de Davos.

[Le Monde] En Somalie, les chababs interdisent Internet dans les zones qu'ils contrôlent

Dans un communiqué paru le mercredi 8 janvier, les insurgés islamistes somaliens ont annoncé le bannissement de l'usage d'internet dans les zones du pays sous leur contrôle : « Toutes les compagnies de communication qui fournissent des services Internet par téléphone ou câble optique en Somalie ont quinze jours pour arrêter leur service ». Toute personne fournissant ou utilisant les services sera ensuite considérée comme "travaillant pour l'ennemi et traité conformément à la charia".

[Thehackernews] Les services de renseignement indiens vont mettre en place NETRA, un projet de surveillance d'Internet

Signifiant "œil" en Hindi, NETRA (Network Traffic Analysis) serait capable de détecter et d'enregistrer toute conversation suspecte s'effectuant par le biais de Skype ou Google Talk. Encore en phase d'expérimentation, le projet devrait être progressivement étendu afin d'intercepter un très grand nombre de données.

[Whitehouse.org] Rapport de la Commission chargée d'étudier la surveillance de la NSA

Le rapport, remis au Président Barack Obama le 12 décembre 2013, a été rédigé par cinq experts suite aux révélations de l'affaire Snowden sur la NSA. Il formule des recommandations qui ont été vivement critiquées par des représentants du renseignement américain.

[Washington Post] Les écoutes téléphoniques de la NSA sont peu efficaces pour prévenir une attaque terroriste selon un rapport

Une analyse menée à partir des dossiers de 225 personnes accusées de terrorisme aux Etats-Unis depuis 2001 a montré que les écoutes téléphoniques réalisées par la NSA sur le territoire national n'avaient "pas d'impact visible dans la prévention d'actes de terrorisme". Dans la plupart des cas, ce sont les investigations des enquêteurs qui se révèlent efficaces pour découvrir les tentatives d'attentat et les réseaux djihadistes. Selon le Director of National Intelligence, James Clapper, ces écoutes permettraient de mieux visualiser les réseaux djihadistes en liens avec l'individu arrêté, de mieux estimer la menace, et donc une plus grande - selon les termes de Clapper - "tranquillité d'esprit" pour les agences officielles.

Capacités de lutte informatique offensive américaines : historique, organisation et perspectives

Le début de l'année 2013 a été marqué par un éclairage mis sur le US CYBERCOMMAND et l'utilisation de ses capacités offensives dans un contexte marqué par les révélations sur le ver Stuxnet et un discours très fort des représentants officiels américains à l'attention de l'Iran et de la Chine. Un an plus tard, l'US CYBERCOMMAND a été effacé par les révélations en cascades d'Edward Snowden sur la National Security Agency américaine (NSA). Or, il convient de rappeler que les deux institutions sont intimement liées et, entre autres, dirigées par le même officier général.

Il existe une synergie entre le renseignement d'origine électromagnétique que collecte la NSA et les capacités de lutte informatique que possède l'US CYBERCOMMAND: le renseignement pouvant fournir les éléments nécessaires au développement des capacités de lutte informatique offensives, et ces dernières pouvant collecter des informations sensibles dans le cadre des opérations de Computer Network Exploitation (CNE). Les capacités de lutte informatique sont développées afin de permettre aux Etats-Unis de mener des cyberattaques (Computer Network Attacks -CNA), améliorer leur cyberdéfense (Computer Network Defense - CND) ou exploiter des réseaux informatiques tiers (Computer Network Exploitation - CNE) .

Fin 2013, les opérations de la NSA ont fait l'objet de vives critiques et d'un discours du Président Barack Obama le 17 janvier 2014 sur une réforme du renseignement d'origine électromagnétique américain. La forte visibilité de la NSA, les critiques formulées et le départ du général Alexander, actuel directeur de la NSA et de l'US CYBERCOMMAND pourraient introduire des changements dans l'organisation de la lutte informatique offensive américaine. Dans ces conditions, il convient de se demander quelle est l'organisation actuelle des capacités de lutte informatique offensives américaines, particulièrement sous l'angle de leur synergie avec la NSA, et quelles sont les perspectives pour 2014 alors que le budget de l'US CYBERCOMMAND a été doublé par rapport à 2013.

Les capacités de lutte informatique américaines ont connu un fort développement depuis la fin des années 1990, avec un tournant résolument offensif en 2009. Quels sont aujourd'hui les développements en cours et les perspectives pour la lutte informatique offensive américaine?

Genèse des capacités de lutte informatique américaines

- **La prise de conscience de la vulnérabilité américaine (1997-2001)**

Du fait de l'utilisation croissante des technologies de l'information dans le domaine militaire, les Etats-Unis prennent conscience dès la fin des années 1990 que les cyberattaques représentent des armes efficaces et attractives pour leurs adversaires.

Plusieurs éléments contribuent à cette prise de conscience. Tout d'abord, la cyberattaque de mai 1999 baptisée *Moonlight Maze*[1] et attribuée à la Russie, qui a visé la NASA, le Pentagone et d'autres agences gouvernementales américaines. Ensuite, le déroulement de deux exercices de simulations, *Eligible Receiver* en juin 1997 et *Zenith Star* en octobre 1999[2], lancés par le Pentagone avec des équipes de la NSA, qui font également prendre conscience de la vulnérabilité américaine liée à sa supériorité technologique, mais aussi du manque de coordination des agences gouvernementales pour la protection du territoire national. En effet, les deux exercices et la cyberattaque ont mené à la paralysie de nombreuses agences et services publiques sur le sol américain. Le *National Security Council*, qui avait pour mission d'appuyer la communauté du renseignement, est mis en cause en juin 2001 par James Adams pour les mauvais résultats des exercices de simulations. Il est alors mis en lumière le manque de moyens financiers, des capacités et des compétences militaires nécessaires pour répondre aux attaques et coordonner les actions entre les agences gouvernementales.

La « normalisation » des opérations dans le cyberespace apparait donc comme une nécessité: dès 1998, le Pentagone créé le *Joint-Tak Force – Computer Network Defense* (JTF-CND), ancêtre du US CYBERCOMMAND. Deux ans plus tard, cette unité se verra confier les missions défensives et offensives.

- **Rapprochement entre secteurs privés et publics et renforcement des actions coordonnées (2003-2006)**

A partir de 2003, unes série d'intrusions dans les serveurs de la défense et d'agences gouvernementales américaines est découverte. Les cyberattaques, regroupées sous le nom de *Titan Rain*[3], sont attribuées à la Chine. L'administration Bush valide en février 2003 le programme de cyber protection du *National Strategy to Secure Cyberspace* et appelle, dans ce contexte, au renforcement de la coopération entre le secteur privé et le secteur public. Dans son article dans *Foreign Affairs en 2001,* James Adams plaidait déjà pour l'adoption d'une stratégie cohérente pour combattre les cyberattaques et le développement d'une défense effective pour garantir la sécurité nationale. Il insistait sur le fait que ce développement ne pouvait être envisagé sans une coopération des agences gouvernementales avec le secteur privé.

Ainsi, dès 2004, la NSA se voit d'abord attribuer les opérations de lutte informatique offensive[4]. Au cours de l'année 2005, cette dernière et l'entreprise *Booz Allen Hamilton* se sont rapprochées à travers la personne de John J. McConnell ce qui a permis – entre autres – à la NSA d'acquérir des capacités cyber venant du secteur privé.

- **Opération Olympic Games et poursuite de la montée en puissance (2006 - 2009)**

En juillet 2009, une cyberattaque massive a ciblé des agences gouvernementales américaines ainsi que certaines entreprises. Sous la forme d'un déni de service distribué (DDoS), l'attaque émanait d'un ou plusieurs

[1]Identifiée par le *Department of Defense.* Washington découvre que ces installations militaires et systèmes gouvernementaux ont subi le vol de nombreuses données, dont des informations potentiellement classifiées portant sur des codes maritimes et systèmes de guidages de missiles.

[2]Lancées au Pentagone à la demande du chef d'état-major interarmes afin de mettre à l'épreuve les capacités civiles et militaires face à une cyberattaque. *Eligible Receiver*: Une équipe désignée pour le piratage, la *Red Team*, a été chargée de mener les attaques est parvenue à paralyser le système de Command-and-Control de la marine, en utilisant simplement le matériel disponible dans le commerce et les informations disponibles sur le web, avec interdiction de violer la législation américaine.

[3]http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management

[4]http://rpdefense.over-blog.com/the-future-of-us-cyber-command

Botnets d'ordinateurs infectés qui se sont "autodétruits" en effaçant leur système d'exploitation une fois l'attaque terminée. Si l'attaque n'a pas pu être attribuée comme ce fut le cas pour *Titan Rain* et *Moonlight Maze*, elle a renforcé l'impression de vulnérabilité des Etats-Unis[5] et motivé la montée en puissance du renseignement d'origine électromagnétique des capacités de lutte informatique américaines.

Les capacités de renseignement d'origine électromagnétique ont connu un fort développement depuis 2001. Si les interceptions des communications "upstream" sont menées par la National Security Agency depuis sa création, le début du programme PRISM en 2007 est un élément important de ce développement car il est le premier programme à collecter à grande échelle les données stockées sur les serveurs des géants d'Internet américains (selon une méthode "downstream"). Ce programme permet à la National Security Agency de collecter des données directement dans les serveurs d'entreprises américaines. En juin 2013, neuf d'entre elles faisaient partie du programme: Microsoft, Yahoo, Google, Facebook, Paltalk, Youtube, Skype, AOL et Apple. Au moment des révélations d'Edward Snowden, Dropbox[6] devait être ajouté au programme. A titre d'exemple, Microsoft aurait fourni à la NSA et au FBI sa clé de chiffrement, permettant aux deux agences d'accéder aux données stockées sur Skydrive et d'intercepter les appels passés sur Skype. Les accords avec les entreprises participant au programme sont également financiers, la NSA remboursant les frais que les entreprises doivent engager pour se mettre en accord avec le cadre juridique du programme. Il existe une forte synergie entre le renseignement d'origine électromagnétique et les capacités de lutte informatique: le premier pouvant fournir les éléments nécessaires au développement des secondes, et les secondes pouvant obtenir des informations dans le cadre des opérations de Computer Network Exploitation (CNE).

En matière de lutte informatique offensive, le début de l'opération Olympic Games témoigne, a posteriori, des avancées effectuées par les Etats-Unis dans la lutte informatique offensive. Le ver informatique Stuxnet, découvert en 2010 par une société de sécurité informatique Biélorusse, a été conçu pour affecter les systèmes SCADA iraniens, plus particulièrement ceux de la centrale d'enrichissement de l'uranium de Natanz. Sa première version date de 2006[7]; il aurait été conçu conjointement par les Etats-Unis et Israël dans le but de ralentir le programme nucléaire militaire iranien. Stuxnet est considéré comme la première "cyber arme" de par son niveau de sophistication élevé et ses objectifs politiques clairement identifiables. La première version de Stuxnet avait pour caractéristique principale la furtivité et pouvait être vue comme "expérimentale". S'il causait des dommages aux centrifugeuses, ceux-ci restaient limités afin de ne pas attirer l'attention. 50% des coûts de conception du ver auraient été dédiés à la furtivité, et ce de manière effective puisqu'en 2009 - lorsque la seconde version de Stuxnet est apparue - la première version n'avait toujours pas été détectée.

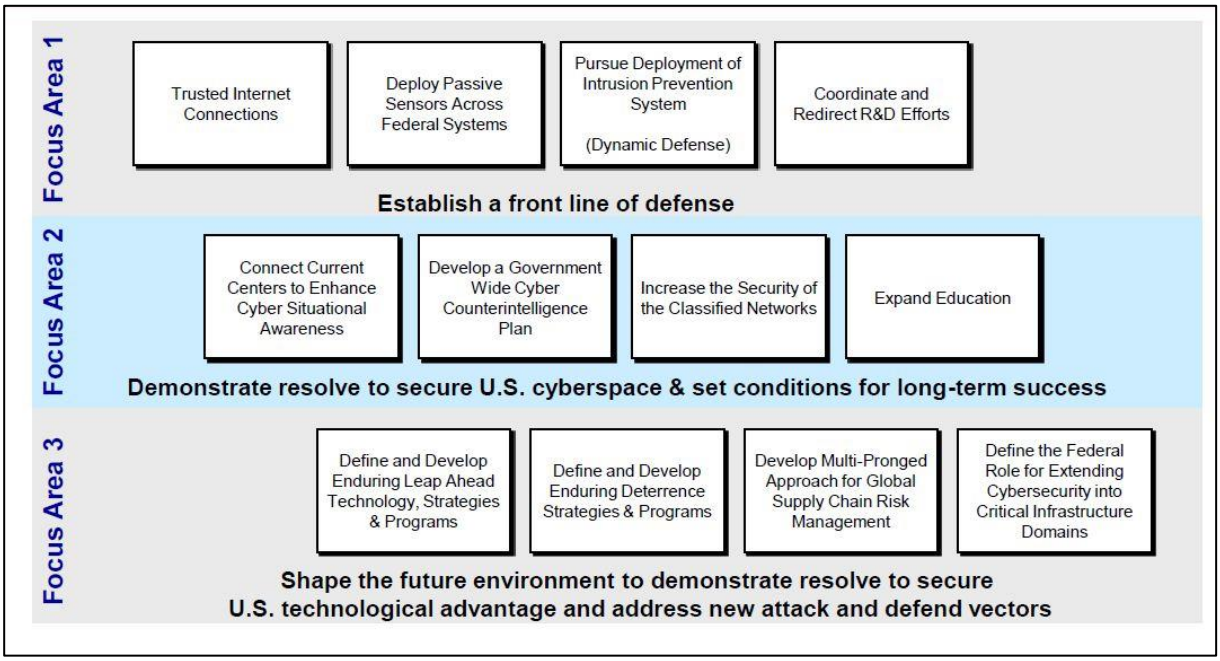
Premier aboutissement de cette montée en puissance, l'année 2009 a été marquée par de nombreux évènements qui en font un tournant pour les capacités de lutte informatique américaines.

Le tournant de 2009

Les capacités de lutte informatique ont connu un fort développement depuis l'élection du Président Barack Obama en 2008, et le tournant résolument offensif en matière cyber qui a suivi son entrée en fonction. Si le début du programme *Olympic Games* décrit par le journaliste américain David Sanger[8] a débuté sous le mandat du Président Georges W. Bush, plusieurs éléments contribuent au tournant de 2009.

[5] http://publicintelligence.net/
[6] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[7] http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
[8] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

- L'adoption en 2008 de la *President's Comprehensive National Cybersecurity Initiative* (CNCI)[9] qui met en lumière l'importance que revêtent les enjeux cyber à travers trois nouveaux défis: la mise en place d'une "ligne de front" de la cyberdéfense, la démonstration d'une volonté de sécuriser le cyberespace sur le long terme, et de développer des technologies qui assureront durablement la supériorité des Etats-Unis face aux futures menaces.

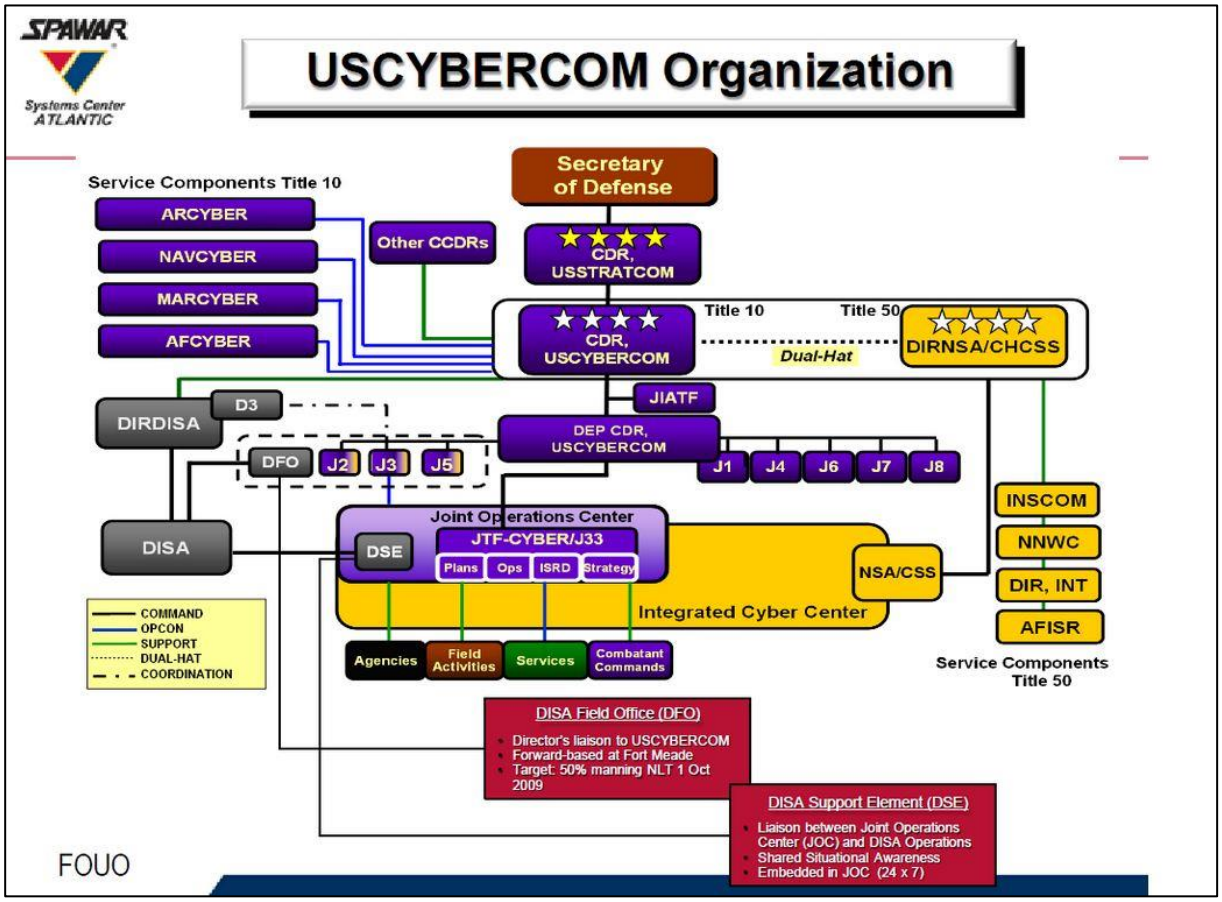


- Ce premier texte de 2008 a ensuite été suivi *du Cybersecurity Act* de 2009[10]qui a augmenté les pouvoirs de plusieurs agences sur Internet, et lancé les premières réformes en matière de cybersécurité des infrastructures critiques.

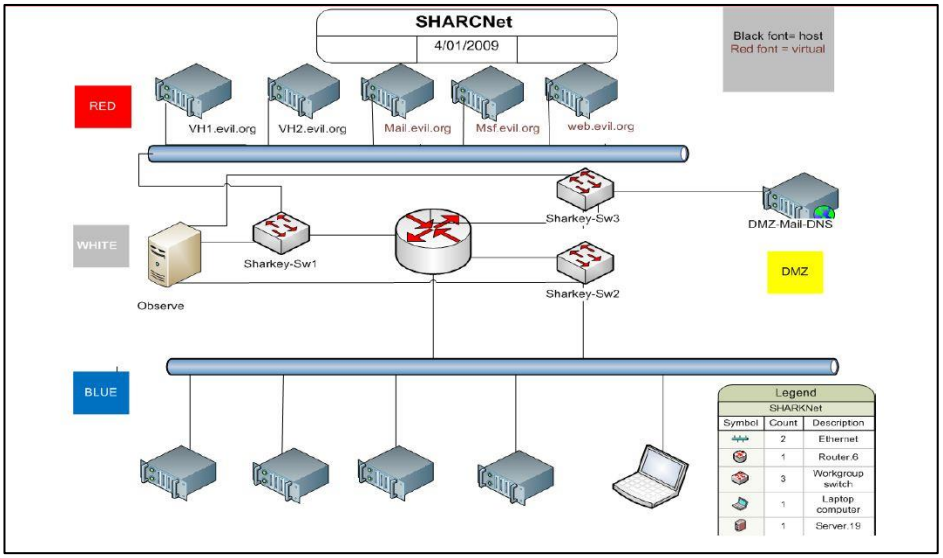
- La création d'une seconde version de Stuxnet en 2009[11], plus destructrice mais moins discrète que la précédente version de 2006, fait également partie de ce tournant. Cette seconde "édition", de par les dégâts qu'elle devait causer et son mode de propagation, avait plus de chance d'être détectée et de désigner les Etats-Unis comme les premiers concepteurs d'une cyber arme majeure.

- La mise en place de l'US CYBERCOMMAND[12] en 2010, et la nomination du directeur de la NSA[13] à sa tête, a eu un fort impact. Ce dernier a été amplifié par l'insistance des représentants officiels sur les capacités de lutte informatique offensive de l'US CYBERCOMMAND, ainsi que sur l'importance de ses effectifs (4000 personnes).

[9] http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
[10] https://www.eff.org/deeplinks/2009/04/cybersecurity-act
[11] http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack
[12] http://online.wsj.com/news/articles/SB124579956278644449
[13] http://www.nsa.gov/about/leadership/bio_alexander.shtml



- La construction la même année du *Cyber Warfare, Exploitation and Information Dominance* (CWEID)[14] Lab avait également pour but de favoriser le développementde technologies de pointe pour la cyber guerre et la cyber sécurité.



[14] http://publicintelligence.net/

- Au sein de ce laboratoire, la *Structured Holistic Attack Research Computer Network (SHARCNet)* - également commandée en 2009 - permet de tester les opérations d'attaque, de défense et d'exploitation de réseaux informatiques tiers (respectivement Computer Network Attacks, Defense and Exploitation).

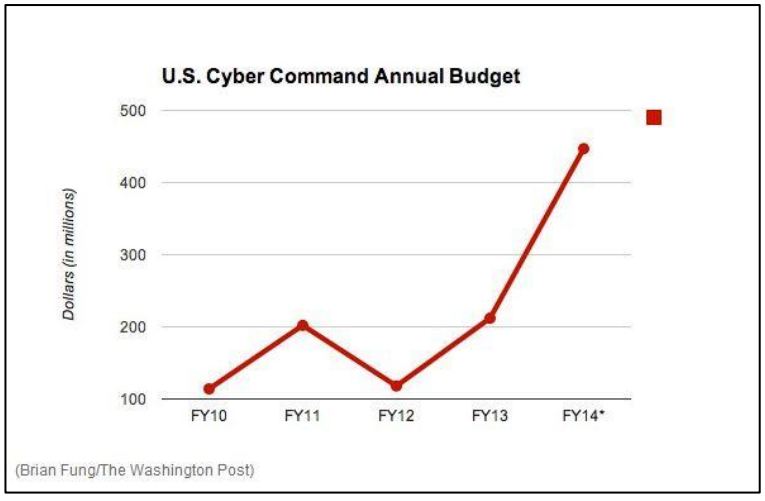
- L'appropriation des questions de cyberdéfense par les représentants de l'Etat[15], qui insistent sur l'importance des enjeux, sur la gravité des attaques qui pourraient frapper le territoire national, et sur le niveau de sophistication croissant des capacités offensives nationales.

Le tournant de 2009 est l'aboutissement d'une montée en puissance entreprise depuis la fin des années 1990, et le signe d'une volonté politique de s'investir plus avant dans le développement des capacités de lutte informatique, avec un accent mis sur l'offensive. Le US CYBERCOMMAND est officiellement en charge de mener les opérations de lutte informatique offensive, tandis que chaque branche de l'armée américaine développe son "propre" CYBERCOMMAND tourné vers la cyberdéfense. Cependant, cette distinction a entraîné une inégalité entre les capacités cyber dont dispose le US CYBERCOMMAND appuyé directement par les capacités de renseignement de la NSA, et celles des forces cyber au sein des armées. Comme le soulignait le général Alexander en avril 2013[16], cette inégalité est source de vulnérabilités qu'il convient de limiter en mettant en place des "Cyberteams" entraînées à la fois pour l'attaque et la défense.

La forte médiatisation de la NSA au cours de l'année 2013 pourrait affecter indirectement l'organisation de la lutte informatique offensive américaine, en remettant en question la double direction de la NSA et du US CYBERCOMMAND, ou en accélérant des réformes de l'organisation des forces cyber américaines en 2014.

Développements en cours et perspectives

Les budgets du US CYBERCOMMAND ont connu une forte augmentation globale depuis la création de l'institution en 2010, et ce malgré une baisse en 2012. Le 14 janvier 2014, la Chambre des Représentants américaines a voté le doublement des budgets alloués à l'US CYBERCOMMAND pour l'année 2014, les faisant passer de 212 millions de dollars à 447 millions de dollars[17].



[15] http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html
[16] http://www.afcea.org/content/?q=node/11117
[17] http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/

Cette augmentation conséquente des budgets devrait permettre la montée en puissance des capacités de lutte informatique américaines précédemment décrites, et pourraient également servir aux grands projets et réformes en cours.

- **Le Joint Information Environment (JIE), une ambition limitée**

En 2013, plusieurs officiers généraux américains ont plaidé pour la mise en place progressive d'un Joint Information Environment (JIE)[18] qui permettrait d'augmenter le niveau de cyber sécurité au sein des forces armées. Le JIE n'est pas un programme et n'a pas de budget alloué. C'est une construction qui va progressivement mener à un réseau unique, global, améliorant l'efficacité opérationnelle, l'interopérabilité et les communications. Il est l'aboutissement d'une série de mesures qui ont été initiées depuis deux ans et qui s'intensifient à l'heure actuelle. Parmi celles-ci, la limitation des points de connexion entre les réseaux du DoD et internet, ou la mise en place de capacités défensives aux points critiques, devraient améliorer la marge de manœuvre des forces américaines dans le cyberespace. Ces capacités défensives se basent, entre autres, sur un filtre de contenu, une passerelle de sécurité pour les e-mails, et d'autres senseurs *« combinant renseignement en temps réel et logiciels pouvant agir sur la base de ces renseignements, (nous) permettant ainsi d'ajuster la posture de défense en anticipation des menaces »* (Major General John Davis).

Cinq mesures constituent « l'ADN » du Joint Information Environment selon Anthony Valletta[19] : **l**a normalisation des réseaux**,** la consolidation de plus de 2000 Datacenters au sein du Department of Defense, la mise en place d'une méthode unique d'identification et de gestion des accès**, l**a mise à disposition de services pour les entreprises au sein du Cloud et la formulation d'une seule et unique politique de gouvernance sur le Joint Information Environment.

Si le projet de JIE est ambitieux, son "ADN" pourrait en définitive se voir considérablement appauvri en 2014 et ne se limiter qu'à la consolidation et colocalisation de Datacenters afin de faciliter leur entretien et leur protection.

- **Le développement des Cyber Teams**

Le général Alexander a insisté sur l'importance du développement de cyber teams spécifiquement formées et habilitées pour mener des opérations de lutte informatique. 40 équipes de ce type devraient être opérationnelles d'ici 2015. 13 d'entre elles être exclusivement consacrées à la réalisation de Computer Netwok Attacks (CNA)[20]. A travers la constitution des cyberteams, les Etats-Unis cherchent à la fois à créer des équipes spécialement entraînées et dédiées à la lutte informatique, et remonter les capacités de cyberdéfense considérées comme inférieures aux capacités de cyberattaques.

- **Une possible réforme de la double direction NSA - CYBERCOMMAND**

En 2013, les révélations d'Edward Snowden sur la *National Security Agency* ont amené une remise en question du fonctionnement de la NSA, et de la double direction NSA-CYBERCOMMAND jusqu'à maintenant assurée par un seul officier général, le général Alexander. Comme l'explique l'amiral Stavridis, un choix doit souvent être fait entre renseignement et action militaire. Afin de surmonter cette difficulté, une "estimation pertes/profits en matière de renseignement" ("intelligence gain/loss assessment") est effectuée par une

[18] http://events.jspargo.com/cybercom13/public/enter.aspx

[19] Anthony Valletta, ancien "acting assistant secretary of defense for command, control, communications and intelligence"

[20] http://www.washingtonpost.com/world/national-security/pentagon-creating-teams-to-launch-cyberattacks-as-threat-grows/2013/03/12/35aa94da-8b3c-11e2-9838-d62f083ba93f_story.html

autorité de haut niveau, un arbitre qui décide du maintien des opérations de renseignement ou de l'autorisation d'une action militaire pouvant les mettre en péril. Or, la double direction NSA - US CYBERCOMMAND a donné un rôle à la fois opérationnel et d'arbitre à l'officier général à la tête des deux institutions[21]. C'est donc le trop grand pouvoir donné à ce dernier qui a été critiqué dans le cadre des révélations de la NSA, mais également l'organisation actuelle de la NSA et de l'US CYBERCOMMAND qui va à l'encontre de la doctrine militaire standard en recherchant une synergie entre les opérations de renseignement d'origine électromagnétique et la lutte informatique américaine. Il existe également un déséquilibre entre un US CYBERCOMMAND ayant à peine quatre ans, et une NSA historiquement ancrée et qui a connu un très fort développement au cours des dernières années. La séparation des deux directions pourrait permettre à l'US CYBERCOMMAND de se renforcer sans être dans l'ombre de la NSA, mais perdre de la synergie sur laquelle insiste le général Alexander. La séparation des deux institutions a été rejetée par le Président Barack Obama en décembre 2013, et n'a pas été abordée dans son discours du 17 janvier sur la réforme du renseignement d'origine électromagnétique américain.

- **La création de forces cyber "indépendantes"**

A l'heure actuelle, chaque service de l'armée américaine dispose de son propre CYBERCOMMAND. Ces forces s'ajoutent à l'US CYBERCOMMAND qui est lui interarmées et directement sous l'autorité du commandement stratégique américain. Dans un article paru en janvier 2014, l'amiral Stavridis plaide pour la création de forces cyber américaines sur le modèle des forces spéciales et de leur commandement, Special Operations Command (SOCOM). Cette réforme pourrait faciliter l'entraînement et la coordination de forces cyber américaines indépendantes des armées et également avoir un impact sur l'US CYBERCOMMAND[22].

[21] http://www.foreignaffairs.com/print/137356
[22] http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force

Découvrez le portail OMC. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

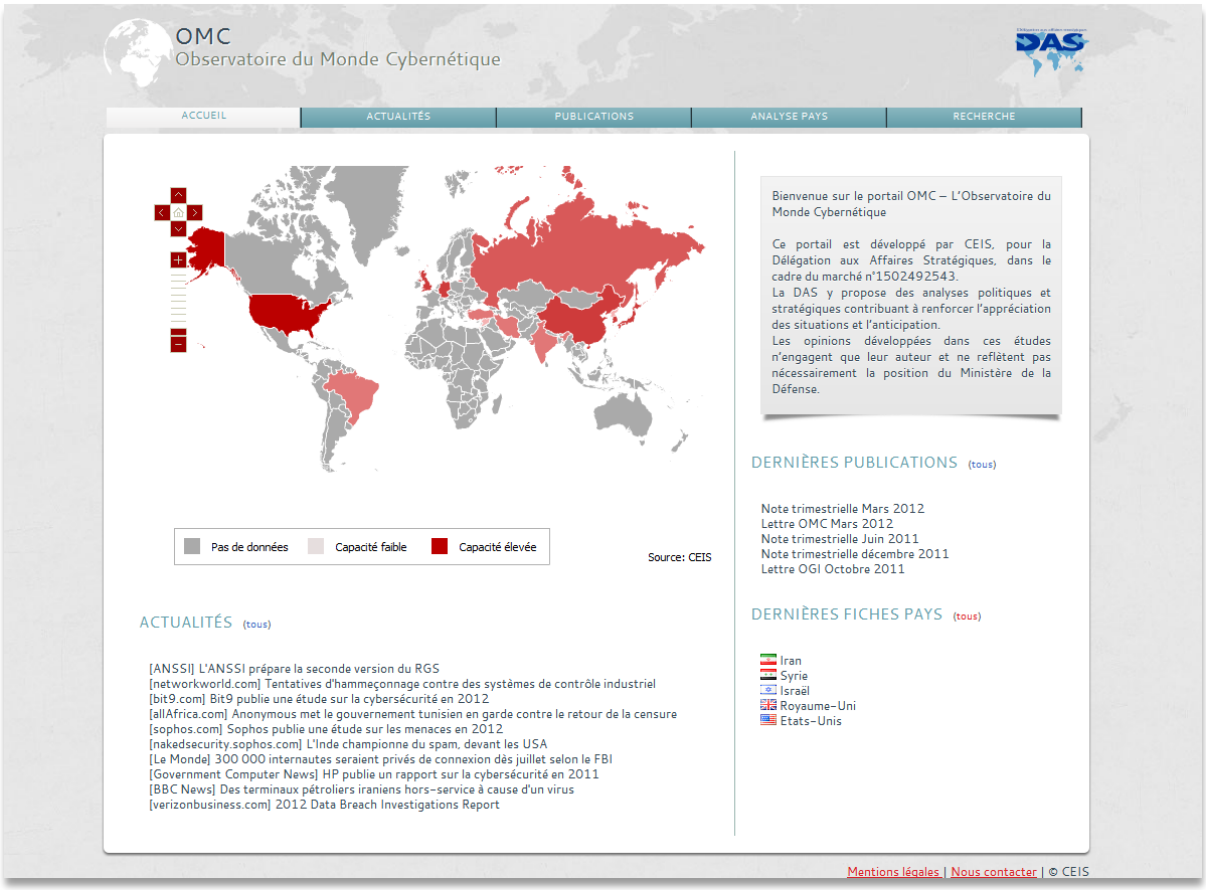


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

Pour vous y connecter, n'hésitez pas à demander vos identifiants à CEIS.

Contact : Barbara Louis-Sidney - blouis@ceis.eu et omc@ceis.eu

Les débats Qualys Security Community	Paris	4 février
Dîner-débat, le cercle européen de la sécurité et des systèmes d'information	Paris	13 février
RSA Conférence 2014	San Francisco	24 - 28 février
CEBIT 2014	Hanovre	10 - 14 mars
Cyber Intelligence Asia 2014	Singapour	11 - 14 mars
ITMeetings, palais des festivals et des Congrès de Cannes	Cannes	19 - 20 mars
Black Hat - Asie	Singapour	25 - 28 mars
3ème congrès national de la sécurité des SI de Santé	Le Mans	31 mars
Cloud Computing World Expo	Paris	9 - 10 avril

CEIS

Compagnie Européenne
d'Intelligence Stratégique

Téléphone : 01 45 55 00 20
Télécopie : 01 45 55 00 60
E-mail : gtissier@ceis.eu

Les opinions exprimées dans cette lettre n'engagent que la responsabilité de leurs auteurs.

Retrouvez cette lettre et l'ensemble des articles cités sur le portail
https://omc.ceis.eu/
(Accès soumis à authentification)

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.

Ministère de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07