Observatoire du Monde Cybernétique

Mars 2012

L'ANSSI adopte une nouvelle organisation

L'ANSSI a annoncé sa réorganisation interne afin de mieux répondre aux problématiques de cyberdéfense et aux menaces liées à la sécurité informatique. Cette nouvelle structure entrera en vigueur le 2 avril.

La société VUPEN ne dévoilera pas sa technique d'exploitation de Google Chrome

VUPEN, société française fondée par Chaouki Bekrar, a passé six semaines à exploiter une vulnérabilité 0-day dans le navigateur Google Chrome, et en a fait la démonstration lors de la compétition *Pwn2Own 2012*. VUPEN ne dévoilera cependant pas sa technique car elle en fait précisément son cœur de métier. Leurs clients, gouvernements membres de l'OTAN et partenaires, payent un abonnement de 100 000 € par an pour avoir un accès exclusif au catalogue d'exploits 0-day proposé par VUPEN.

Lancement d'un centre de lutte européen contre la cybercriminalité

La Commission européenne a proposé le lancement d'un pôle européen de lutte contre la cybercriminalité, fléau qui coûterait jusqu'à 388 milliards d'euros par an. Sa mission principale sera de protéger les citoyens contre l'usurpation d'identité et le piratage sur les réseaux sociaux.

ACTA : le Parlement européen ne saisira pas la Cour de justice

Le Parlement européen a rejeté une proposition du rapporteur David Martin lui recommandant de soumettre l'Accord commercial anti-contrefaçon (ACTA) à la CJUE. M. Martin devra par conséquent réitérer sa proposition initiale, et ce avant le 26 avril 2012. La décision finale de la commission du commerce sera rendue les 29 et 30 mai prochains.

L'OTAN signe un contrat sur la cyberdéfense

L'OTAN a signé un contrat avec certains acteurs privés (comme Finmeccanica et Northrop Grumman) pour augmenter ses capacités de cyberdéfense. Ce contrat permettra à la *NATO Computer Incident Response Capability* (NCIRC) d'arriver à pleine capacité opérationnelle à la fin 2012, et permettra aux Etats membres de bénéficier d'une aide pour se défendre en cas de cyberattaque.

Locked Shields 2012 : l'exercice de cybersécurité de l'OTAN.

L'OTAN a organisé le 26 mars un exercice de lutte informatique multilatéral. Etaient opposées deux équipes dans un scénario de gestion de crise, comprenant aussi une composante technique : une *Red Team* composée de participants estoniens et finlandais, contre une *Blue Team* plus nombreuse, avec des participants de Suisse, Allemagne, Espagne, Finlande, Italie, et des alliances Autriche-Allemagne, Danemark-Norvège, ainsi qu'une équipe de l'OTAN. L'exercice voulait mettre l'accent sur la communication inter-équipes.

Les Etats-Unis veulent que le DoD soit le garant de leur cyberespace

Les législateurs américains sont en train de défendre l'idée que la cyberdéfense devrait relever de la responsabilité du Département de la défense (*Department of Defense*) et non du Département de la sécurité intérieure (*Department of Homeland Security*), qui est actuellement chargé de protéger les infrastructures sensibles du pays. Ceci permettrait aux Etats-Unis de se prémunir contre des attaques externes plus rapidement, sans attendre que le DHS les considère comme des actes de guerre pour donner le feu vert au DoD.

Le gouvernement américain est en train de perdre la guerre contre les *hackers*

D'après Shawn Henry (assistant au directeur général du FBI), la méthode avec laquelle le gouvernement américain se défend actuellement contre les cyberattaques n'est pas durable. Le niveau des attaquants serait trop élevé par rapport aux mesures défensives mises en place. Shawn Henry préconise un changement urgent dans le comportement des entreprises et dans leur manière d'aborder la sécurité. Le *status quo* est, d'après lui, la meilleure manière de ne « jamais être sécurisé ».

La NSA construit son plus grand centre d'écoute

D'après une enquête menée par le magazine *Wired*, la *National Security Agency* américaine a commencé la construction d'un *datacenter* géant dans la ville de Bluffdale, dans l'Utah. Ce complexe aura une surface de 92 900 m² et sera le plus grand nœud du réseau informatique de la NSA. Le coût de la construction est estimé à 2 milliards de dollars. Afin de préserver le caractère secret des informations qui y circuleront, une zone désertique et reculée a été choisie comme emplacement de ce nouveau centre qui devrait être opérationnel en septembre 2013.

La NASA piratée plusieurs fois pendant les deux dernières années

La NASA a fait l'objet de plusieurs attaques informatiques pendant ces deux dernières années. L'une d'entre elles a permis aux pirates d'accéder au *Jet Propulsion Laboratory* de l'agence. D'après le compte rendu à la *House Science, Space, and Technology Subcommittee*, les adresses IP associées à l'attaque se trouvaient en Chine. En 2011, la NASA a dû faire face à 47 attaques de type APTs, dont 13 auraient réussi à pénétrer leurs systèmes informatiques.

Le Pentagone décidé à accélérer sa R&D en matière de cyberarmes

Afin de se prémunir d'éventuelles confrontations avec l'Iran ou la Syrie, le Pentagone américain a décidé d'accélérer ses efforts de développement de cyberarmes de nouvelle génération, capables de nuire aux réseaux militaires ennemis, même sans que ceux-ci ne soient connectés à Internet. Les dépenses totales du Pentagone en capacités de cyber s'élèvent à 3,4 milliards de dollars cette année.

La DARPA investit en recherche cyber-offensive

La *Defense Advanced Research Projects Agency* (DARPA) commencera à financer de la recherche en capacités de lutte informatique. 246 millions de dollars seront alloués exclusivement à la recherche en sécurité informatique. Le directeur du DARPA, Ken Gabriel, estime que les tactiques de guerre moderne exigent une capacité d'attaque matérielle mais aussi cybernétique, d'où l'importance des investissements.

Le *leader* du groupe LulzSec collaborait avec le FBI

En juin 2011, Hector Xavier Monsegur, le *leader* du groupe des *hackers LulzSec*, a été secrètement arrêté et a commencé à collaborer avec le FBI. Selon le communiqué de presse du FBI du 6 mars 2012, cette collaboration a permis à l'agence fédérale d'arrêter cinq autres membres du groupe.

***AnonymousOS* et *Slowloris* se retournent contre leurs utilisateurs**

Suite au lancement *d'AnonymousOS*, une version *d'Ubuntu* recensant plusieurs outils de sécurité informatique, les canaux « officiels » *d'AnonOps* ont démenti tout rapport avec la création d'un tel système. *AnonymousOS* contiendrait en effet, en plus de la panoplie classique d'outils de sécurité, plusieurs chevaux de Troie qui pourraient être extrêmement nuisibles à son utilisateur. Une version de *Slowloris*, un des outils de DDoS collaboratif utilisés par les personnes affiliées au mouvement *Anonymous*, a notamment été piratée et détournée pour déclencher l'installation d'un cheval de Troie, *ZeuS*. Ce *malware* a pour principales fonctionnalités de dérober les coordonnées bancaires de l'utilisateur, ainsi que ses mots de passe et cookies web.

Un réseau criminel utilisant *Carberp* a été démantelé

Le 20 mars 2012, la police russe a annoncé l'arrestation d'un gang de cybercriminels impliqué dans le vol d'argent en utilisant le cheval de Troie *Carberp*. Il ne s'agissait cependant que de simples utilisateurs du réseau et non de ses créateurs. Les auteurs du *malware* sont toujours en liberté, et vendent ouvertement le cheval de Troie sur les « *black markets* » en ligne.

Un Général américain confirme l'origine du piratage de RSA

Le Général américain Keith Alexander a confirmé publiquement la responsabilité de la Chine dans l'attaque du système *SecurID* de RSA. Plusieurs chercheurs en sécurité informatique avaient décelé des indices qui désignaient ce pays comme origine probable. Selon Keith Alexander, la facilité avec laquelle le système RSA a été compromis montre bien la vulnérabilité potentielle des autres entreprises, ce qui pourrait encourager les *hackers*

organisés et soutenus par un Etat à mener des attaques plus fréquentes.

L'Autriche et la Russie renforcent leur coopération dans la lutte contre la cybercriminalité

L'Autriche et la Russie ont décidé de renforcer leur coopération pour la lutte contre la cybercriminalité, en prévoyant de créer une unité de cybersécurité de haut niveau. Une conférence ministérielle aura lieu à cet égard en avril 2012 à Vienne avec la participation des membres de l'Union européenne, la Russie et les États-Unis.

L'Australie lance son premier concours national de cybersécurité

Le gouvernement australien organise la première compétition nationale de la cybersécurité, le *Cyber Defence University Challenge 2012*. Le but principal de l'événement est d'évaluer les compétences des étudiants en informatique et en cybersécurité. Selon Stephen Conroy, le ministre australien des communications et de l'économie numérique, ce concours permettrait de « sensibiliser les universitaires à l'importance de la cybersécurité, tout en présentant des débouchés pour les jeunes diplômés en TIC ».

[verizonbusiness.com] 2012 Data Breach Investigations Report

Verizon Business a publié son rapport d'enquête sur les compromissions de données. Selon les chercheurs, plus de la moitié (58%) des données volées en 2011 étaient le résultat d'un acte de nature cyber-activiste. Plus de 90% de ces attaques auraient pu être évitées, contre seulement 4% ayant été classées comme étant particulièrement difficiles à prévenir. Les experts soulignent également que les cybercriminels sont de plus en plus impliqués dans l'espionnage industriel.

[INSA] Cloud Computing : Risks, Benefits, and Mission Enhancement for the Intelligence Community

Le rapport publié par l'*Intelligence and National Security Alliance* détaille comment le *Cloud computing* affecterait la gestion et le business model des *datacenters* des agences de renseignement. Le changement de rythme qu'apporte le *Cloud computing* permettra aux agences de réagir plus rapidement et leur donnera la possibilité de lancer des programmes en deux ans plutôt qu'en cinq ans ou plus. De plus, du fait de la nature décentralisée de l'architecture en *cloud*, les données collectées entre agences seront plus facilement partagées.

[USCC] Occupying the Information High Ground : Chinese Capabilities for Computer Network Operations and Cyber Espionage

Northrop Grumman a rédigé un rapport pour la *U.S.-China Economic and Security Review Commission* montrant une recrudescence des tests offensifs dans le cyberespace de la part des forces militaires chinoises. D'après le rapport, *« les capacités chinoises en matière d'opérations réseaux ont beaucoup progressé et représenteraient un risque réel pour les unités opérationnelles américaines dans le cas d'un conflit »*.

[SANS] The Jester Dynamic : A Lesson in Asymmetric Unmanaged Cyber Warfare

Le rapport publié par le SANS Institute examine l'impact qu'un pirate « électron libre » a eu au cours des deux dernières années, et les leçons à en tirer, afin de mieux se prémunir contre des attaques de ce type.

[BlueCoat] Blue Coat Systems 2012 Web Security Report

Blue Coat Systems, Inc. a publié son rapport « Blue Coat Systems 2012 Web Security Report » qui identifie et analyse les tendances des cyberattaques en 2011. D'après les spécialistes, une des grandes tendances 2011 est l'apparition de réseaux de logiciels malveillants (*malware network* ou *malnet*). D'après le rapport, le nombre de sites malveillants a augmenté de 240 % en 2011. L'étude traite également les stratégies employées pour la manipulation des *malnets*, ainsi que le comportement des utilisateurs et les outils de défense.

[Imperva] The Anatomy of an Anonymous Attack

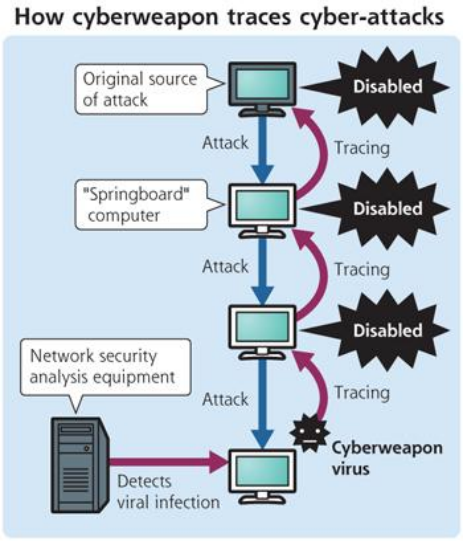
Le groupe de cyber-activistes *Anonymous* a tenté d'attaquer le site web du Vatican, sans succès. Le système informatique du Vatican possédait en effet des composants capables d'enregistrer les actions des attaquants. Ceci a permis à la société gérant la sécurité de leur SI - Imperva - de produire un rapport détaillant de près l'organisation, son échéancier, et les méthodes type d'une attaque *d'Anonymous*.

[PWC] Fighting Economic Crime in the Financial Services sector

PricewaterhouseCoopers a publié un rapport sur l'impact de la cybercriminalité sur les entreprises. *«La cybercriminalité est mondiale et les frontières géographiques traditionnelles n'offrent aucune protection. Les entreprises doivent posséder une bonne connaissance des menaces cybernétiques actuelles et émergentes, et les dirigeants doivent comprendre les risques et les possibilités associés au cyberespace.»*

Cyber-arme japonaise et course à l'armement informatique

Le Japon a été la cible en 2011 de nombreuses cyber-attaques (cyber-espionnage et attaques par déni de services distribué). Ses ambassades durant l'été, son Parlement en octobre et surtout l'un des principaux fournisseurs des forces armées japonaises, Mitsubishi Heavy Industries (MHI), un conglomérat industriel (spatial, aéronautique, énergie, construction navale, etc.) ont été les principales victimes de cette série d'attaques informatiques.



Suite à ces évènements, la presse japonaise[1] a commencé à évoquer en janvier 2012 un projet de développement d'une cyber-arme destinée aux forces armées d'autodéfense japonaises. Selon le journal Yomiuri Shimbun, ce projet aurait démarré en 2008 pour un budget d'environ 2,3 millions de dollars (179 millions de yens). Fujitsu serait chargé de développer cette cyber-arme « défensive » capable de « tracer, identifier et de désactiver les sources de cyber-attaques ». Cette arme informatique serait testée dans un environnement confiné. Interrogée par les journalistes, la société n'a pas souhaité réagir à ce sujet.

La publicité organisée autour de ce projet sensible soulève néanmoins plusieurs questions**.**

Qu'est-ce qu'une cyber-arme ?

Peut-on réellement qualifier le projet japonais d'arme informatique ? Une cyber-arme peut être définie comme un programme informatique malveillant dont la finalité est de pénétrer les réseaux informatiques adverses pour compromettre ou saboter son système d'information ou un sous-ensemble de celui-ci.

Stuxnet, la première cyber-arme ?

Stuxnet est souvent présenté comme l'exemple « parfait » de ce qui peut être défini comme une cyber-arme. Très sophistiqué (c'était la première fois qu'on détectait un programme informatique malveillant exploitant quatre failles 0-day combinées à des certificats numérique volés), Stuxnet semble avoir été développé par un ou plusieurs Etats dans un but unique : ralentir le programme nucléaire iranien en sabotant les centrifugeuses d'enrichissement d'uranium.

Une cyber-arme ne peut néanmoins pas être simplement définie par sa seule complexité. D'autres programmes malveillants comme les RAT (*Remote Administration Tool*) ou les logiciels permettant de coordonner et lancer des attaques par déni de service distribué peuvent être également qualifiés de cyber-armes. Il faut également souligner le caractère dual d'une arme informatique. En effet, un seul et même programme informatique peut être à la fois être développé et utilisé à des fins défensives ou offensives, et dans un contexte militaire ou civil.

[1] http://www.yomiuri.co.jp/dy/national/T120102002799.htm

Certains auteurs comme Thomas Rid et Peter McBurney proposent également une classification[2] des cyber-armes en deux grandes catégories :

- Les armes informatiques génériques à faible potentiel. Elles sont comparées à du paint-ball. Elles sont simples d'utilisation, facilement disponibles mais leurs impacts restent limités (par exemple, des malwares basiques, des outils DDoS, etc.)

- Les armes informatiques sur-mesure à haut potentiel. Elles sont comparées à des armes « intelligentes ». Très sophistiquées, elles nécessitent une phase spécifique de renseignement sur les systèmes ciblés, des investissements importants en matière de R&D et un temps de développement élevé (par exemple, Stuxnet ou Duqu[3]).

L'efficacité des cyber-armes reste encore en débat. Si développer une cyber-arme possède des avantages (coût, furtivité, difficulté à identifier l'attaquant), les utiliser présente plusieurs difficultés (nécessité d'un niveau de renseignement technique très précis sur les cibles, fiabilité incertaine, effets collatéraux, généralement à usage unique). Stuxnet, par exemple, a été détecté sur des centaines de milliers de machines aux quatre coins du monde, alors que sa cible principale était le programme nucléaire iranien.

La première utilisation d'une cyber-arme dans un contexte militaire peut également se révéler problématique car un raté est hautement probable, à l'instar du premier emploi d'une arme classique. De ce fait, son emploi tactique sur les théâtres d'opération reste encore incertain et il semblerait aujourd'hui que l'usage d'une arme informatique doive obligatoirement être couplé à des armes plus anciennes. La fiabilité et les effets des cyber-armes restent en effet à prouver.

Quel est le cadre légal de ce type de développement ?

Au Japon, développer un programme informatique malveillant est interdit. Le développement et, de fait, l'utilisation de cette cyber-arme serait donc impossible en théorie. Mais pour en permettre l'exploitation, la loi devrait être modifiée ou la définition légale d'une arme pourrait être revue. Se pose également la question de la légalité de l'utilisation d'une telle cyber-arme contre un pays étranger dans le cadre du droit international.

La riposte, en droit international, ne peut se concevoir que suite à une agression armée [3, f), résolution 3314, ONU]. Mais ce schéma est difficilement transposable à la cyberattaque. Comment prouver que l'on est en présence d'une agression armée pour justifier la riposte ? Comment passer outre les problèmes d'intensité de l'attaque et d'attribution ?

Pour toutes ces raisons, la cyberattaque sera le plus souvent employée de façon discrète et anonyme, à des fins de cyberespionnage par exemple. Elle pourra également être utilisée en préparation ou appui d'une opération militaire plus classique.

Le volet offensif de la cyber-arme (en projet) chargé de localiser puis de « neutraliser » l'attaquant entre également en conflit avec le statut particulier des forces d'auto-défense japonaises. En effet, depuis 1945, le Japon ne dispose que d'une armée défensive, lui interdisant tout comportement offensif.

[2] http://www.tandfonline.com/doi/full/10.1080/03071847.2012.664354#tabModule

[3] Pour en savoir plus : http://www.numerama.com/magazine/20466-le-virus-duqu-detecte-par-un-outil-open-source.html

Quelle crédibilité donner à ce projet ?

A l'instar d'autres pays, le Japon semble développer ses capacités défensives et offensives de lutte dans le cyberespace en testant des cyber-armes. Ces dernières ont pour objectif de lui permettre de se défendre mais aussi et surtout de riposter en cherchant à « désactiver les sources des cyber-attaques ». Le budget supposé du projet (2,3 millions de dollars) reste relativement faible, ce qui confirmerait le fait que le coût de développement des cyber-armes serait négligeable par rapport aux projets d'armement traditionnel.

Le Japon n'est pas le seul pays à revendiquer le développement de son cyber-arsenal. En juin 2011, le *Washington Post*[4] dévoilait que le Pentagone dispose d'une liste de cyber-armes pouvant être utilisées dans le cadre d'une attaque informatique. Chacune de ces cyber-armes disposerait de procédures opérationnelles associées en clarifiant l'usage (quand et comment les exploiter). La mise en œuvre de certaines de ces cyber-armes semblerait cependant conditionnée à l'aval du président américain (dans le cas des virus notamment), sauf dans les cas de « zones de guerre déclarées » où cette approbation peut être délivrée de façon préalable. D'autres, utilisées à des fins de renseignement pour analyser les capacités de défense des infrastructures critiques, n'auraient pas besoin d'une telle autorisation.

En novembre 2011, la DARPA fait part de son objectif de développer de nouvelles cyber-armes (offensives et défensives) pour mieux protéger les réseaux militaires des Etats-Unis mais également pour avoir la capacité de répliquer. L'agence américaine dépendant du Pentagone en avait profité pour recommander de doubler les financements alloués aux travaux de recherche menés en matière de lutte dans le cyberespace (208 millions de dollars). En février 2012, le Dr. Kaigham J. Gabriel, directeur adjoint de la DARPA, a confirmé, devant le sous-comité « Menaces émergentes et Capacités »[5] de la Chambre des représentants des Etats-Unis, les intentions de l'agence d'accélérer le développement de cyber-armes offensives autant que défensives.

Usage avorté de cyber-armes

En octobre 2011, le *New York Times*[6] dévoile des réflexions menées par les stratèges militaires avant l'intervention en Libye. En effet, selon le journal américain, Washington aurait envisagé de lancer des cyber-attaques contre la Libye pour saboter les défenses anti-aériennes du régime de Kadhafi afin de préparer la mise en place de la zone d'exclusion aérienne prévue par la résolution 1973 du Conseil de Sécurité des Nations Unies. Comme en 2003 avant l'intervention en Iraq[7] , les cyber-attaques n'ont finalement pas été lancées, par crainte de constituer un précédent majeur et de légitimer des actions similaires de la Russie et de la Chine. Ces actions soulèvent pose également des questions juridiques. Aux Etats-Unis, la *War Powers Resolution* oblige le Président américain à informer le Congrès avant de lancer une guerre. Mais cette résolution était-elle requise pour une cyber-attaque ?

[4] http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html?wprss=rss_politics

[5] http://www.armedservices.house.gov/index.cfm/files/serve?File_id=95e7caf8-5918-4afc-9b33-f504b5ca6555

[6] http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=2

[7] http://www.fiercegovernmentit.com/story/u-s-considered-2003-cyber-attack-iraq/2009-08-02

La Grande-Bretagne n'est pas en reste dans ce domaine. En mai 2011, dans une interview donnée au Guardian[8], Nick Harvey, le ministre des forces armées britanniques déclarait : « l'action dans le cyberespace fera partie du futur champ de bataille » il ajoutait que « les cyber-armes font partie intégrante de l'arsenal du pays ». Le GCHQ[9], par l'intermédiaire de son Cyber Security Operations Center, et le Cabinet Office joueraient un rôle majeur dans le développement de cette capacité offensive.

Entre communication et dissuasion

Les projets de développement de cyber-armes ne font pas la une des médias. La plupart des Etats préfèrent en effet ne pas communiquer sur ce sujet, encore très sensible. D'autres pays, comme les Etats-Unis, la Grande-Bretagne ou encore le Japon, semblent ne plus cacher leurs intentions en matière de développement de capacités défensives mais surtout offensives de lutte dans le cyberespace.

La communication autour du développement de cyber-armes américaines vise également à décourager un adversaire potentiel d'attaquer les États-Unis. L'intégration de cyber-technologies est sûrement le développement le plus significatif dans la doctrine « cyber » américaine. Cette communication, distillée à minima, semble parfaitement organisée par les autorités américaines. Les initiatives de communication du Japon et de la Grande-Bretagne suivent cette même logique. Déclarer publiquement détenir des cyber-armes et être prêt à les utiliser revêt une dimension psychologique importante dans un objectif de dissuasion.

[8] http://www.guardian.co.uk/government-computing-network/2011/may/31/government-plans-cyber-weapons-programme
[9] Government Communications Headquarters

Hackito Ergo Sum	Paris	Du 12 au 14 avril
ENISA PPP	Rome	Du 19 au 20 avril
Infosecurity Europe 2012	Londres	Du 24 au 25 avril
BSides London	Londres	Le 25 avril
SANS AppSec Summit	Las Vegas	Du 24 avril 2 mai

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 notre extranet
https://owldesk.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