Observatoire du Monde Cybernétique

Lettre n°26 – Février 2014

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

Le 20 janvier 2014, en envoyant un SMS d'intimidation sur les téléphones de tous les participants aux manifestations contre le gouvernement, l'Ukraine a montré qu'elle détenait des capacités de surveillance sans pour autant atteindre l'effet recherché. Alors que de nombreuses agences de par le monde ont recours à des dispositifs mobiles pour surveiller discrètement les téléphones dans une zone donnée, l'Ukraine se sert au contraire de méthodes héritées de l'époque soviétique et de dispositifs russes implantés massivement dans le pays depuis la fin de l'année 2010. L'exemple ukrainien n'est pas isolé : la plupart des pays de la Communauté des Etats Indépendants ont hérité des méthodes utilisées par le KGB en URSS, et ont progressivement imité la Russie pour mettre en place des systèmes de surveillance de masse.

[LemagIT] L'Anssi poursuit ses travaux sur la sécurisation des infrastructures industrielles

L'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) vient de publier deux documents proposant une méthode de classification des systèmes industriels, ainsi que des mesures permettant de renforcer leur sécurité informatique. Ces documents n'ont "aucune valeur contraignante" mais ont pour but d'aider à l'application des mesures spécifiées dans la Loi de Programmation Militaire adoptée en décembre 2013. Celle-ci vise en particulier au renforcement de la cybersécurité des Opérateurs d'Importance Vitale (OIV).

[Ariase] Orange au cœur de l'écosystème de la cyberdéfense

Lors de son déplacement à l'Ecole des Transmissions de Rennes (ETRS) pour annoncer la mise en place du "Pacte Cyber Défense 2016", le ministre de la Défense Jean-Yves le Drian était accompagné du PDG d'Orange, Stéphane Richard. L'opérateur Télécom Orange est depuis quelques mois au cœur de l'actualité depuis le piratage de près de 800 000 de ses comptes utilisateurs, et du lancement officiel d'Orange Cyberdéfense le 21 et 22 janvier 2014 lors du Forum International de la Cybersécurité.

Au cours de sa visite en Bretagne, le ministre de la Défense a également visité le CyberSOC (Security Operating System) d'Orange Business Service situé à Cesson-Sévigné.

[Pastrèsnet.blog.lemonde.fr] Uhuru, le mobile sécurisé made in France

Le projet de création d'un antivirus français, DAVFI (pour « démonstrateur d'antivirus français et internationaux »), a été rebaptisé Uhuru. Ce dernier est le premier antivirus 100% français développé par Nov'IT, Qosmos, TechLib, le constructeur de navires DCNS et l'école d'ingénieurs ESIEA de Laval. Son développement était essentiel pour des raisons de souveraineté : les antivirus ont en effet accès à l'intégralité du contenu de l'appareil qu'ils protègent, et sont donc potentiellement des vecteurs de surveillance particulièrement efficaces. Uhuru n'est pas un simple antivirus, mais un système d'exploitation qui s'inspire d'Android tout en se voulant à la fois plus sécurisé et open source. Les développeurs ont conservé une fonction de géolocalisation qui n'enverra pas des données relatives au lieu où se trouve le possesseur du smartphone, mais indiquera aléatoirement que ce dernier se trouve au quartier général de la NSA, de la CIA, du FBI, de la DGSE, de la DCRI…

[Numerama] Géolocalisation policière : l'Assemblée adopte un texte plus libéral

Les députés ont adopté le mardi 11 février le projet de loi de géolocalisation qui prévoit que tout type d'objet pourra être géolocalisé afin de suivre un suspect. Alors que le texte voté en Sénat voulait limiter la géolocalisation aux suspects de crimes et délits punis d'au moins 5 ans d'emprisonnement, ou à des cas très restrictifs, l'Assemblée Nationale a voté un texte plus libéral qui autorise la géolocalisation en temps réel pour tout suspect de délits punis par trois ans ou plus d'emprisonnement.

[LesEchos] Piratage informatique : la France ciblée par un Etat étranger ?

Les experts en sécurité informatique de Kaspersky Lab ont révélé l'existence d'un virus informatique du nom de "Careto" en espagnol (la langue apparemment utilisée pour son développement), ou "The Mask" en anglais. Bien plus sophistiqué que les virus normalement conçus par les cybercriminels, le virus aurait permis d'espionner plus de 384 cibles entre 2007 et 2014.

Il aurait ciblé des gouvernements, des missions diplomatiques, des entreprises du secteur énergétique, des organismes de recherche, des sociétés de capitaux privés ou encore des militants politiques. La France serait un des cinq pays les plus touchés par "The Mask". Très sophistiqué, et non encore attribué à un Etat l'heure actuelle, le virus utilisait un moyen de "chiffrement"

sophistiqué lors de l'exfiltration des données recueillies sur les machines infectées.

[Silicon] Contre la NSA, Merkel va proposer à François Hollande de faire réseau commun

La chancelière allemande Angela Merkel a proposé au Président François Hollande la création d'un réseau européen évitant que les données personnelles ne transitent par le territoire américain. Cette proposition s'inscrit dans le cadre de la contre-offensive que mène l'Allemagne contre les Etats-Unis depuis les révélations des écoutes de la National Security Agency qui allaient jusqu'à la surveillance des communications de la chancelière. L'Elysée a par ailleurs confirmé qu'un dialogue à ce sujet était actuellement en cours entre les autorités françaises et allemandes, et ce malgré le fait que le Président français ait joué la réconciliation sur les questions d'espionnage lors de son récent voyage aux Etats-Unis.

[Silicon] Une faille d'Internet Explorer exploitée pour cibler l'aéronautique française

Une faille d'Internet Explorer aurait pris pour cible les adhérents du GIFAS (Groupement des Industries Françaises Aéronautiques et Spatiales). Cette attaque sophistiquée passait dans un premier temps par un faux site du GIFAS qui permettait de récupérer des informations sur les visiteurs, et de les rediriger vers d'autres sites également falsifiés. Une seconde vulnérabilité, de Shockwave Flash cette fois-ci, était ensuite utilisée afin d'accéder aux données contenues sur les ordinateurs des internautes.

[ZATAZ] Attaque informatique via une clinique parisienne

Alors que de nombreux serveurs français et britanniques font l'objet depuis quelques jours d'une attaque massive, notamment dirigée contre le siège des services de renseignement britannique, le Government Central Communications Headquarter (GCHQ), des sites français ont été utilisés dans le cadre d'une attaque par déni de service (DDoS). Parmi ceux-ci, le site Internet de l'Institut de la main a ainsi été utilisé.

[pro.01.net] Inauguration des nouveaux locaux parisiens de l'ANSSI

L'Agence nationale de sécurité des systèmes d'information a inauguré ses nouveaux locaux avec la présence de Jean-Marc Ayrault. C'est dans la Tour Mercure à proximité de la Tour Eiffel que se trouve le centre opérationnel de l'ANSSI, composé de trois zones distinctes, une cellule de veille, un centre de détection et une salle de situation et d'analyse. C'est de là que l'agence détectera les attaques informatiques menées contre les administrations et les entreprises françaises.

[LePoint] Des mesures d'urgence annoncées pour la cybersécurité

Lors de sa visite dans les nouveaux locaux de l'ANSSI, Jean Marc Ayrault a dévoilé plusieurs mesures de Défense. Parmi celles-ci, le Premier ministre a annoncé le chiffrement des messageries proposées par les opérateurs français, ainsi que leur hébergement sur le territoire national. Parmi les autres mesures annoncées, le chiffrement systématique des réseaux de l'Etat, ou encore une responsabilisation des chefs d'entreprise vis-à-vis de leurs systèmes d'informations.

[Lalibre.be] Le génie belge du chiffrement espionné par la NSA

Dans le cadre de l'enquête sur le piratage massif qui a affecté Belgacom, la police belge a découvert qu'un logiciel malveillant avait été installé sur l'ordinateur d'un expert belge de la cryptographie et de la protection des données personnelles, Jean-Jacques Quisquater. Le GCHQ britannique, dont l'espionnage de Belgacom par le biais de la technique "quantum injection" a été révélé en novembre 2013 par des documents d'Edward Snowden, serait également derrière ce piratage. Le procureur fédéral en charge des enquêtes contre l'espionnage a confirmé qu'un dossier a été ouvert sur "l'affaire Quisquater".

[LeMonde] Contre l'espionnage américain, Brésil et Europe veulent leur câble sous-marin

La construction d'un nouveau câble sous-marin entre Lisbonne au Portugal et Fortaleza au Brésil a été décidée lors du septième sommet UE-Brésil organisé à Bruxelles ce lundi 24 février 2014.

Financé par des fonds européens et brésiliens, le câble sera placé d'ici 2015 grâce à un partenariat entre l'entreprise brésilienne de télécommunication Telebras et l'espagnol IslaLink Submarine Câbles. Depuis les révélations sur l'espionnage de la National Security Agency, le Brésil et plusieurs pays européens ont vivement condamné les pratiques américaines et cherché des solutions pour les éviter.

Suite à la révélation de la mise sur écoute du téléphone de la présidente brésilienne Dilma Rousseff et de l'espionnage de l'entreprise pétrolière Petrobras, le Brésil a renouvelé sa volonté de construire des câbles ne passant pas par le territoire américain.

En Europe, la chancelière allemande Angela Merkel avait proposé, avec le Brésil, une résolution aux Nations Unies qualifiant les programmes de surveillance de masse de la NSA de « violation des droits de l'homme et des libertés ». Elle s'était également prononcée en faveur d'un Internet européen afin de se soustraire à l'espionnage américain.

[Defense.gov] Le DoD annonce la nomination du directeur du nouveau commandant du Cyber Command/directeur de la NSA

Le Secrétaire à la Défense américain Chuck Hagel a annoncé le 30 janvier la nomination du vice-amiral Rogers à la tête du US Cyber Command et de la NSA. Ancien commandant du Cyber Command des forces navales américaines, Rogers va succéder au général Alexander en poste depuis 2005 à la NSA, et depuis 2010 au US Cyber Command.

La nomination doit encore être validée par le Congrès américain. La nomination du nouveau directeur adjoint de la NSA, Richard Ledgett, a également été faite par la même occasion. Richard Ledgett était précédemment à la tête d'une équipe spéciale chargée de la gestion des fuites d'informations occasionnées par Edward Snowden. Lors d'une interview, il avait qualifié ces fuites de "cataclysmiques" et avait tenté par plusieurs actions de redorer l'image de la NSA à travers des actions de transparence.

[TheVerge] Le piratage de la US Navy par les iranien a été plus étendu et plus invasif qu'annoncé

En septembre 2013, le plus large réseau non confidentiel d'ordinateurs de la Navy a été piraté par un groupe "travaillant directement pour l'Iran ou agissant avec le soutien des leaders iraniens".

Selon le Wall Street Journal qui a révélé l'attaque, le groupe a visé le réseau de la Navy Marine Corps en utilisant une faille de sécurité dans un des sites Internet public de la marine américaine. Bien que, selon les déclarations officielles, l'attaque n'ait pas permis aux iraniens de mettre la main sur des documents classifiés, l'attaque a néanmoins été plus étendue et plus invasive que prévue.

Les iraniens n'ayant jusqu'en septembre utilisé que des attaques par Déni de Service Distribué (DDoS) contre le gouvernement américain, les autorités avaient déclaré avoir été surprises du niveau de sophistication de l'attaque. Il aura ainsi fallu quatre mois pour que les équipes du Navy Cyber Command parviennent à purger le réseau de toute infection. Le Navy Cyber Command est toujours dirigé par le futur successeur du général Alexander au US Cyber Command, le vice-amiral Rogers.

[JornalDiaDia] Amorim a annoncé son projet d'école de cyberdéfense

Le ministre brésilien de la Défense, Celso Amorim, a annoncé qu'un groupe de travail avait été mis en place pour créer une Ecole Nationale de Cyberdéfense. Des budgets à hauteur de 40 millions de dollars auraient été débloqués pour sa création, et afin de former à terme des "professionnels du domaine de la cyberdéfense".

[UPI] La Russie va mettre en place une unité de cyberdéfense

Le major général Yuri Kuznetsov a déclaré à RIA Novosti qu'une unité de cyberdéfense serait "prête à défendre les infrastructures critiques des forces militaires russes" d'ici 2017. Les cyberattaques sont une préoccupation croissante des autorités russes qui ont mis en place un cybercommand en décembre 2013.

En ce qui concerne la société civile, une autorité officielle en charge de la lutte contre la cybercriminalité a annoncé que les cyberattaques avaient coûté 28 millions en 2013 aux citoyens russes.

[Bloomberg] Israël va créer une équipe de réaction contre les cyberattaques

Le National Cyber Bureau israélien devrait mettre en place en 2014 une équipe de réaction cyber spécialisée dans la réponse aux cyber attaques et pouvant intervenir pour soutenir les entreprises et les citoyens en cas de crise. La création de cette équipe s'inscrit dans un plan plus large de sensibilisation à la cybersécurité en Israël, visant à améliorer les échanges entre acteurs de la société civile et les instances officielles en charge de la cyberdéfense.

[LesEchos] La cybersécurité israélienne suscite les convoitises

Le salon International CyberTech qui s'est tenu les 27 et 28 janvier à Tel Aviv a montré à quel point la Valley Israélienne mise sur la cybersécurité. Cette dernière a vu naître de nombreux experts en cybersécurité, dans un pays qui compte 224 sociétés dans le secteur de la protection de données. Le secteur de la cybersécurité israélienne a connu une forte croissance au cours de ces dernières années, croissance qui devrait se poursuivre avec l'implantation de grandes multinationales. IBM va ainsi ouvrir un "centre d'excellence" israélien spécialisé dans la sécurité et la protection des installations stratégiques. Lockheed Martin devrait quant à lui lancer un centre de recherche et développement en matière de cybersécurité en association avec le spécialiste du stockage informatique EMC. Les deux centres seront localisés dans le cyber-parc de Be'er Sheva où est déjà implanté Deutsche Telecom.

[Si-Vis.blogspot.fr] Le Japon lance son premier "jour de la cybersécurité" et renforce sa coopération avec l'Inde et les USA

Le 3 février 2014 a eu lieu au Japon la première journée nationale consacrée à la cybersécurité. Elle s'inscrit dans une volonté d'améliorer la cybersécurité du pays face aux menaces cyber grandissantes dans la région. Le Japon a également adopté l'année dernière un plan de cybersécurité 2015 - 2020, et renforcé sa collaboration avec l'Inde et les Etats-Unis dans le domaine. Les Etats-Unis devraient bientôt accueillir et former des militaires japonais à la cyberdéfense.

Les capacités de surveillance de masse russes

"Cher souscripteur, vous êtes enregistré comme participant à un mouvement de perturbation de masse"
(SMS reçu par tous les manifestants en Ukraine le 20 janvier 2014)

Le 20 janvier 2014, en envoyant un SMS d'intimidation sur les téléphones de tous les participants aux manifestations contre le gouvernement[1], l'Ukraine a montré qu'elle détenait des capacités de surveillance sans pour autant atteindre l'effet recherché. Alors que de nombreuses agences à travers le monde ont recours à des dispositifs mobiles[2] pour surveiller discrètement les téléphones dans une zone donnée, l'Ukraine se sert au contraire de méthodes héritées de l'époque soviétique et de dispositifs russes implantés massivement dans le pays depuis la fin de l'année 2010.

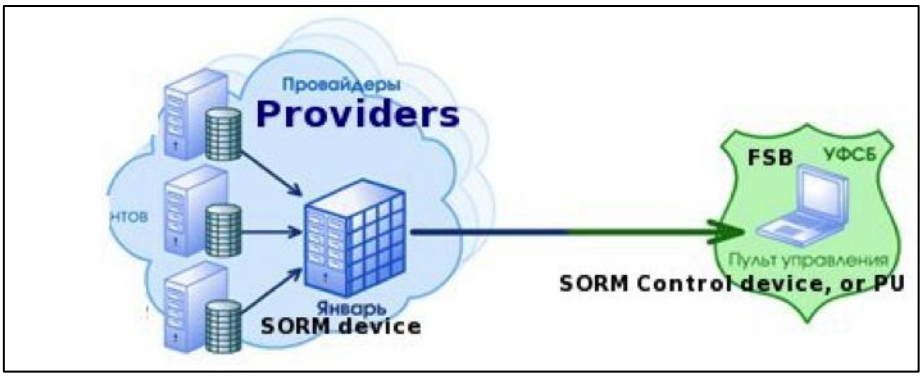
Les opérations de surveillance des télécommunications, appelées *Operativno-Rozisknie Meropriatiya* (ORM), étaient menées dès le début des années 1960 en URSS par le département technique du KGB. En 2014, le terme ORM est toujours utilisé par les autorités ukrainiennes pour qualifier les opérations de surveillance des télécommunications menées sur le territoire national à l'aide de méthodes et de technologies transmises par le *Federal Security Bureau* (FSB) russe[3]. L'exemple ukrainien n'est pas isolé : la plupart des pays de la Communauté des Etats Indépendants ont hérité des méthodes utilisées par le KGB en URSS, et ont progressivement imité la Russie pour mettre en place des systèmes de surveillance de masse.

SORM, le système de surveillance de masse russe

SORM (*System for Operative Investigative Activities*)[4] est employé par le FSB pour surveiller la totalité des communications sur le territoire Russe. Il se décompose en trois parties qui ont progressivement émergé avec l'apparition de nouveaux moyens de communication. SORM-1 a tout d'abord été mis en place en 1996 pour surveiller les communications téléphoniques, et a ensuite été complété dès 1999 par SORM-2 en ce qui concerne les communications sur Internet. Enfin, avec un périmètre d'action plus large, SORM-3 collecte des données sur les autres moyens de communication.

Les opérateurs télécom russes sont tenus de mettre en place dans leurs installations et à leurs frais les dispositifs nécessaires au bon fonctionnement de SORM. Le FSB est directement relié à ces installations par des câbles souterrains qui maillent le pays, et qui lui permettent de mener une surveillance des communications en temps réel. La totalité des données stockées sur les serveurs des opérateurs télécom est accessible au FSB sous réserve de délivrance d'un mandat que les agents ne sont plus tenus de dévoiler.

[1] http://techcrunch.com/2014/01/22/ominous-text-message-sent-to-government-protestors-in-ukraine/
[2] http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/
[3] http://www.theguardian.com/law/2014/jan/21/human-rights-watch-report-criticises-nsa-mass-surveillance
[4] http://www.worldpolicy.org/journal/fall2013/Russia-surveillance



SORM est connecté aux serveurs des opérateurs télécom - privacyinternational.org

Les interceptions de communication téléphonique et par Internet ont explosé au cours des dernières années, passant de 265 937 en 2007 à 539 864 en 2012, tandis que les alertes faites aux opérateurs télécom pour non-respect des dispositions relatives à l'application de SORM[5] sont passées de 16 à 30 par an dans le même laps de temps.

Une surveillance régionale

Si SORM n'est implanté qu'en Ukraine, Biélorussie, Ouzbékistan, Kirghizistan et Kazakhstan[6], tous les pays de la Communauté des Etats Indépendants ont adopté un outil développé par des programmeurs russes qui permet de faire des recherches dans les données à disposition. Baptisé *Semantic Archive*, ce programme vient en complément de SORM et permet, à la manière de *Xkeyscore*[7] pour les Etats-Unis, d'effectuer des recherches ciblées dans les serveurs des services ou des opérateurs télécom.

Une tendance au renforcement

Alors que l'accès aux données contenues dans les serveurs situés sur le territoire national est quasi-total, la Russie s'inquiète des données stockées à l'étranger[8] auxquelles elle n'a pas accès. Le rôle joué par les réseaux sociaux dans les révolutions arabes et dans les manifestations massives en Russie en décembre 2011 n'a depuis fait que renforcer cette inquiétude.

Le contexte actuel de défiance envers les géants d'Internet américains pourrait faciliter l'adoption de mesures les contraignant à stocker les données personnelles des citoyens russes sur le territoire national, et ainsi renforcer les capacités de surveillance du FSB tout en s'alignant sur les mesures que souhaitent adopter de nombreux pays indignés par l'espionnage de la *National Security Agency* (NSA). L'organisation des Jeux Olympiques d'hiver à Sotchi a également permis à la Russie de mettre en place une surveillance à très grande échelle, notamment en exploitant le réseau de l'opérateur télécom russe Rostelecom qui fournit gratuitement Internet à toute la ville depuis début 2013. Le contexte actuel semble donc en faveur du renforcement de capacités de surveillance déjà en forte croissance.

[5] https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach
[6] https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach
[7] http://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html
[8] http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Le portail OMC
La plateforme de la DAS

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

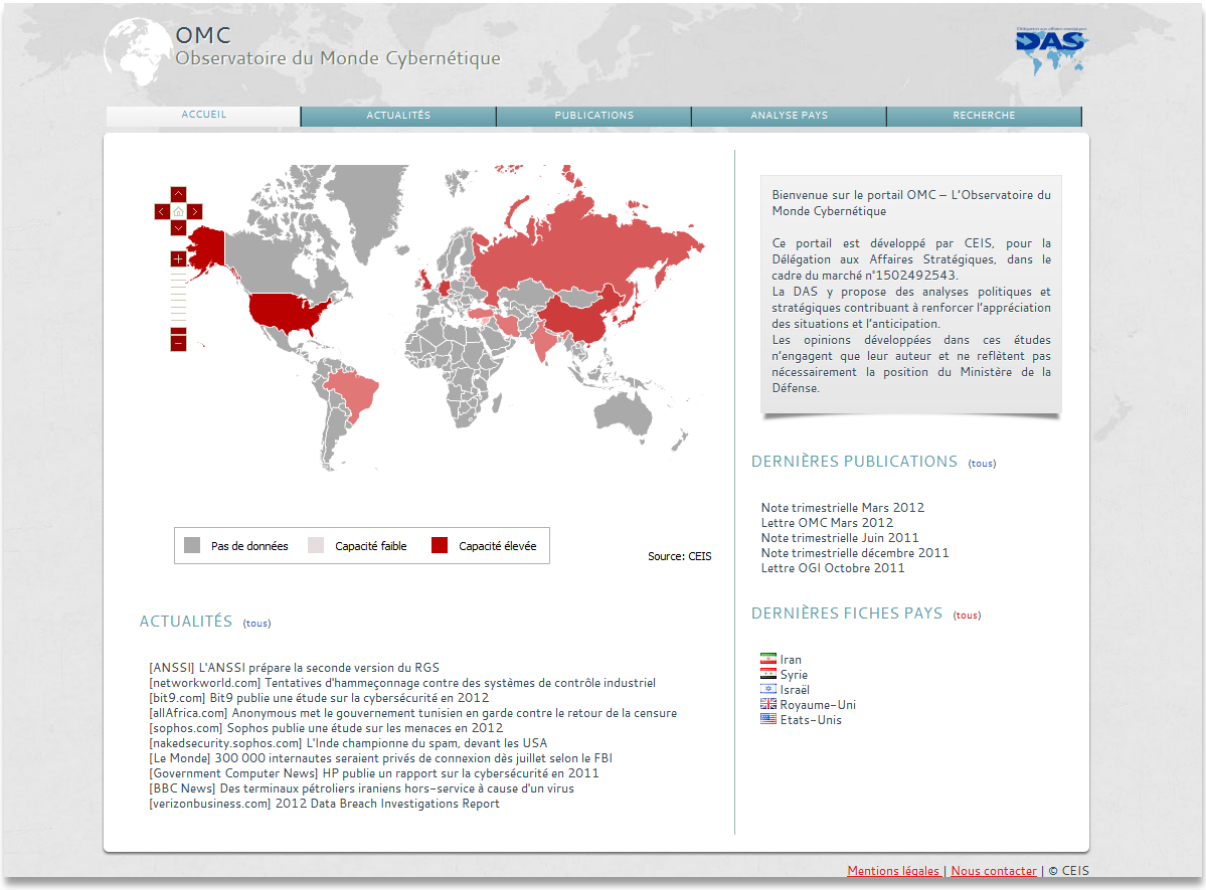


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

Ce portail est réservé au ministère de la Défense et aux administrations qui en feront la demande.

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

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

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
IT Night	Paris	24 mars
Black Hat - Asie	Singapour	25 - 28 mars
3ème congrès national de la sécurité des SI de Santé	Le Mans	31 mars
Symposium on Security for Asia Network	Singapour	31 mars
Cloud Computing World Expo	Paris	9 - 10 avril
2014 World Conference on Information Systems and Technologies (WorldCIST 14)	Madeira	15 avril
The Third International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2014)	Beyrouth	29 avril
EUROCRYPT 2014	Copenhague	11 mai
Infiltrate 2014	Miami	15 mai

CEIS

Compagnie Européenne
d'Intelligence Stratégique

Téléphone : 01 45 55 00 20
Télécopie : 01 45 55 00 60

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