Observatoire du Monde Cybernétique

Lettre n°20 – Aout 2013

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

A l'occasion de sa conférence sur l'aviation qui se déroulait du 11 au 13 août 2013, l'Institut Américain de l'Aéronautique et de l'Astronautique a publié un guide pour la cybersécurité dans l'aviation intitulé *Le Défi de la connectivité : protéger les actifs critiques dans un monde connecté. Un cadre pour la cybersécurité dans l'aviation*.

Lors de la DEF CON 21, la société Lookout a présenté son travail d'enquête sur l'industrialisation des virus sur mobile en Russie. Baptisée « Dragon Lady », cette opération témoigne de la grande organisation de ces réseaux, au point que 60% des virus observés par Lookout soient générés par un noyau d'une dizaine d'entreprises russes, de véritables grossistes du malware SMS.

Début août 2013 le FBI dévoilait son nouveau portail, iGuardian, offrant la possibilité aux entreprises de rapporter les cyberattaques dont elles ont été victimes ou les failles en matière de cybersécurité ayant été découvertes. Retour sur ce modèle de coopération public-privé dans la lutte contre la cybercriminalité.

[CNIL] Notification de violation de données personnelles : nouvelle téléprocédure

Elargissant le spectre de l'obligation de notification de violations de données à caractère personnel, le règlement européen du 24 juin 2013 relatif aux failles de sécurité imposait aux autorités de protection des données de mettre à disposition un moyen électronique sécurisé dédié.

Pour répondre à cette exigence, la CNIL vient de mettre en place une nouvelle téléprocédure sur son site Internet.

[Numerama] Thierry Breton (Atos) veut un « Schengen des données personnelles »

L'ancien ministre de l'économie Thierry Breton, désormais PDG du groupe Atos, veut défendre l'idée de créer une forme d'espace Schengen pour la circulation des données personnelles. Comme pour l'espace Schengen, la régulation se ferait aux frontières de cet espace mais serait inexistante en son sein.

Thierry Breton défendra cette idée auprès du président de la République François Hollande vendredi 30 août à l'Elysée, puis au près de la chancelière allemande Angela Merkel quelques jours après.

[LeFigaro] Les hackeurs, cibles convoitées des recruteurs

Pour connaître les failles de leurs systèmes, les entreprises n'hésitent plus à faire appel aux hackers. Contrairement aux ingénieurs informaticiens classiques, un hacker testera la sécurité de l'installation du point de vue du pirate.

Si la communauté de hackers regorge d'autodidactes, cette absence de diplôme ne freine cependant pas leur recrutement, réalisé grâce au networking en ligne, via des conférences, des concours ou tout simplement leur réseau.

[Le Monde] L'Allemagne reconnaît le Bitcoin pour mieux le taxer

L'Allemagne a annoncé la reconnaissance officielle de la monnaie virtuelle comme « monnaie privée ». Grâce à ce statut juridique, tous les échanges multilatéraux pourront être réalisés dans cette devise virtuelle en Allemagne. En contrepartie, l'administration fiscale pourra prélever une taxe sur toutes ces transactions.

[ZD Net] Création d'un cyberlaboratoire pour soutenir la lutte contre la cybercriminalité

En Inde, un laboratoire d'expertise informatique va être ouvert afin de soutenir la police dans ses enquêtes en matière de cybercriminalité.

[JDN] Quelles sont les nouvelles menaces pour la sécurité des entreprises fournisseurs de services énergétiques ?

La sécurité informatique devient toujours plus complexe, au point que l'approche traditionnelle consistant à établir un périmètre de sécurité autour de l'entreprise ne suffit plus. Les Smart Grids font apparaître de nouveaux problèmes de sécurité : sécurité matérielle des équipements, des systèmes informatiques, de communication, d'acheminement et de traitement des données, confidentialité des données. Le risque existe que les logiciels, les compteurs et autres équipements des sociétés de services énergétiques puissent être infectés par des programmes malveillants, en phase de fabrication et de transport.

[ABC] Janet Napolitano craint une cyberattaque majeure contre les Etats-Unis

La secrétaire démissionnaire du Department of Homeland Security (DHS), Janet Napolitano, a laissé à son successeur encore à désigner une lettre ouverte l'alertant des menaces pesant sur les Etats-Unis et indiquant les travaux à poursuivre. Selon elle, le danger le plus présent est celui d'une cyberattaque massive aux conséquences graves sur les vies, l'économie et le fonctionnement quotidien

de la société américaine. Janet Napolitano occupait ce poste depuis 2009.

[ANInews] Etats-Unis : les académies militaires veulent intégrer la cyberdéfense dans leurs cursus

Selon le Washington Times, une nouvelle étude a révélé que les académies militaires américaines se battent pour intégrer les problématiques cyber dans leurs formations, qui ne contiendraient à l'heure actuelle aucune notion sur le sujet.

[Infosecurity] Etats-Unis : l'ex-secrétaire du DHS lance un Conseil de la cybersécurité

Jane Holl Lute, un ancien secrétaire du Département de la sécurité intérieure (DHS) a annoncé le lancement d'un Conseil de la cybersécurité, une ONG destiné à dégager des bonnes pratiques et à remédier au déficit d'experts en la matière.

[InfoDSI] En 2012, le coût des violations de données s'élève à 2,86 M€

Selon la 4ème édition de l'étude « Cost of Data Breach », publiée par Symantec Corp et le Ponemon Institute, le coût des violations de données a augmenté de 11 % en 2012, pour s'établir à 2,86 millions € contre 2,55 millions € en 2011. Le coût moyen par donnée compromise s'élève à 127 € en 2012, contre 122 € en 2011, soit une augmentation de 4,1 %.

[WallStreetJournal] L'internet chinois frappé par une cyberattaque massive

La Chine a connu au cours du weekend des 24-25 août sa plus grande attaque en déni de service. Confirmée par les officiels du pays, l'attaque a visé le système DNS du pays, privant quantité d'internautes chinois d'accès à internet pendant plusieurs heures. Le China Internet Network Information Center, l'autorité chinoise en la matière, a présenté ses excuses et a expliqué que la panne était le fait de deux attaques consécutives, dont l'origine et les motivations restent inconnues.

[ZD Net] Le Bangladesh durcit les peines en matière de cybercrimes

Un projet de loi réformant la loi sur les technologies de l'information et de la communication a été approuvé par le gouvernement du Bangladesh. Il prévoit la possibilité d'arrêter des auteurs de cybercrimes sans mandat et augmente la peine encourue à 14 ans de prison. La destruction de données avec intention criminelle, le transfert de données sans autorisation ou l'intrusion seront désormais des crimes.

[RiaNovosti] L'armée russe se dote d'une force de cyberguerre

L'armée russe vient de créer au sein de ses forces une branche spécialement dédiée à la cyberguerre afin de pouvoir répondre aux cybermenaces nationales.

[RT] Russie : une loi pour empêcher l'utilisation de Tor

Le chef de Service fédéral de sécurité a ordonné la préparation d'une loi visant à empêcher le recours au réseau Tor en Russie afin de lutter contre la cybercriminalité.

[Renesys] Cuba : l'accès à internet s'améliore

Depuis la mise en service du câble sous-marin ALBA-1 venant du Venezuela le 14 janvier 2013, 118 cybercafés ont ouverts sur l'île. Plus récemment le gouvernement cubain a annoncé la prochaine mise en place de l'ADSL pour les particuliers.

[Computer World] Le Sénat américain lance une enquête sur les monnaies virtuelles

La commission sur la sécurité nationale et les affaires intérieures a envoyé une lettre au directeur du Département de la sécurité nationale au sujet des monnaies virtuelles. Objectif : amorcer une enquête visant à identifier les procédures et lignes directrices pour traiter des affaires relatives aux monnaies virtuelles.

[ENISA] L'ENISA publie son rapport annuel sur les incidents majeurs au sein de l'UE

L'ENISA a publié mardi 20 août 2013 son rapport annuel sur les incidents les plus fréquents affectant l'Union européenne. Le réseau téléphonique mobile a été le plus touché, avec pour conséquence de rendre l'accès à internet indisponible pour des millions d'utilisateurs.

[GMS] 11,6 % des PC ayant une solution de sécurité sont infectés

Il y a 3 ans, Bitdefender lançait Quickscan, un scanner antivirus qui s'exécute directement depuis le navigateur web. Après analyse et publication des données recueillies, Bitdefender révèle que 11,6 % des ordinateurs scannés à l'initiative de leurs utilisateurs, sont infectés par des malwares alors qu'ils sont protégés par une solution de sécurité. Les données recueillies par QuickScan montrent aussi que le plus grand nombre d'ordinateurs infectés se trouvaient : en Inde (taux d'infection de 14,48%), en Roumanie (11,55%), en France (7,47%), aux États-Unis (5,43%).

[LeMonde] Comment la Chine planifie son réseau Internet pour 2020

Le 12 août 2013, le gouvernement chinois a publié son plan d'action stratégique pour la Chine haut débit avec pour objectif de s'approcher des pays développés en termes d'infrastructures, d'innovation et de compétitivité en 2020. Objectif : atteindre un taux de couverture de l'Internet haut débit fixe de 70 % et un taux de 85 % pour les utilisateurs de l'internet mobile.

[TheDiplomat] Une nouvelle mission de cybersécurité japonaise

Le ministère de la Défense japonais a publié un Rapport Intérimaire de Posture de Défense insistant sur l'importance de développer une coopération nationale et internationale pour améliorer la cyberdéfense japonaise. Le rapport constitue une base de travail pour l'élaboration des nouvelles lignes de conduite du Programme de Défense Nationale, publié fin 2013.

[FireEye] Le malware Poison Ivy est de retour

Selon une étude de FireEye publié jeudi 22 août 2013, le malware Poison Ivy, un logiciel malveillant d'accès à distance, serait de retour. Resté populaire et efficace huit ans après sa première apparition, il a à son actif plusieurs dizaines d'attaques contre des entreprises du Fortune 1000.

[ItalianInstituteofStrategicStudies] Cyberarmes : aspects stratégiques et juridiques

Le think tank italien Instituto Italiano Di Studi Strategici a publié une étude sur les enjeux stratégiques et juridiques des cyberarmes. Le document traite notamment de la responsabilité politique et juridique de l'attaquant. Les chercheurs en appellent également à une définition juridique des cyberattaques et à une évaluation plus précise des cybermenaces, pour normaliser le domaine d'action cyber.

[AllAfrica] Un rapport de la TESPOK kenyane identifie les banques et le VoIP comme principales cibles de cybercriminalité

L'Association des Fournisseurs de Services de Télécommunications Kenyane (TESPOK) a publié un rapport dans lequel elle identifie les principales menaces de cybersécurité pesant sur les entreprises kenyanes. Au sommet de sa liste figurent celles pesant sur le secteur bancaire, et celles exploitant les failles du VoIP.

[MEMRI] La cyberguerre en Iran : des hackers au service du régime

Le Middle East Media Research Institute (MEMRI) a analysé et évalué la préparation du régime iranien sur le plan cyber, en se concentrant notamment sur ses capacités offensives. Dans un rapport synthétisant ses recherches, le MEMRI explique que l'Iran a entièrement reconstruit son système informatique, et s'appuie sur des hackers (recrutés ou soutenus) au service du régime. Ces hackers sont présentés dans le rapport.

Un cadre pour la cybersécurité dans l'aviation

"As one of the most complex and integrated systems of information and communications technology (ICT) in the world, the global aviation system is a potential target for a large-scale cyber attack. With the continual and rapid integration of new technologies, the aviation industry keeps expanding, changing, and becoming increasingly connected. As technologies rapidly evolve, however, so do our adversaries and their threats. Without the appropriate cybersecurity measures in place for this evolving threat, the industry may be at risk. Therefore, it is imperative that the industry maintain the highest levels of confidence in aviation."

A l'occasion de sa conférence sur l'aviation qui se déroulait du 11 au 13 août 2013, l'Institut Américain de l'Aéronautique et de l'Astronautique a publié un guide pour la cybersécurité dans l'aviation intitulé *Le Défi de la connectivité : protéger les actifs critiques dans un monde connecté. Un cadre pour la cybersécurité dans l'aviation*. L'Institut Américain de l'Aéronautique et de l'Astronautique est une association regroupant les professionnels de l'aérospatial qui a pour objectif de répondre aux attentes desdits professionnels et de faire avancer la science, l'ingénierie, la technologie et les politiques publiques sur ces questions[1].

L'aviation est un outil indispensable au commerce et au tourisme internationaux et son impact sur l'économie est estimé à 200 milliards de dollars par an. Elle se caractérise par une interconnexion des réseaux et systèmes d'information et sa gouvernance implique une multitude d'autorités nationales, internationales et associatives. A ce titre, assurer un système sécurisé et sûr est **une responsabilité partagée** entre tous les acteurs et à tous les niveaux, de l'élaboration et de la construction de nouveaux aéronefs à la maintenance de ceux-ci, en passant par le trafic aérien et la communication entre les acteurs. Si l'interdépendance croissante des systèmes d'aviation bénéficie au commerce, elle constitue une cible de choix pour ceux qui cherchent à troubler l'industrie et l'économie globale.

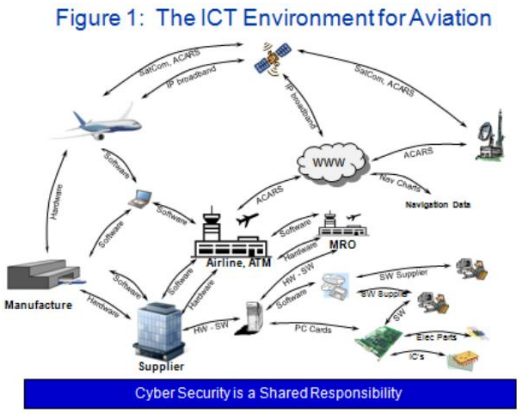


Figure 1. La cybersécurité dans le domaine de l'aviation, une "responsabilité partagée"

[1] http://www.aiaa.org/secondary.aspx?id=153

La multiplication des attaques contre les réseaux et systèmes d'information est un nouvel enjeu pour le monde de l'aviation dont la survie est conditionnée par un niveau élevé de confiance des utilisateurs. Dès lors, l'ensemble des acteurs de l'aérospatial doit travailler à l'émergence d'un cadre pour assurer une cybersécurité optimale des systèmes utilisés. Aujourd'hui, il n'existe pas de standard commun ou de politique internationale définissant le niveau de cybersécurité devant être atteint. L'objectif du document proposé par l'Institut Américain de l'Aéronautique et de l'Astronautique est donc *« d'établir un cadre pour aider la communauté de l'aviation à construire un projet pour assurer que les infrastructures critiques sont sûres et à même de résister et de réagir à des cyberattaques »*[2].

L'Institut Américain de l'Aéronautique et de l'Astronautique suggère que la communauté de l'aviation établisse des **standards communs** pour les systèmes d'aviation ainsi qu'une **culture de la cybersécurité**. Ceci doit passer par une compréhension globale des menaces (qui sont les acteurs, quelles sont leurs intentions) et des risques (quels sont les éléments à protéger, comment les protéger et combien de temps cela prend-il). Il propose que ces connaissances soient partagées avec les autorités nationales sur un forum, comme cela peut se faire pour les infrastructures d'importance vitale, et que des équipes d'ingénieurs en sécurité informatique soient mises en place afin de pouvoir intervenir le plus rapidement possible.

Cependant, l'efficacité des différents dispositifs reposera sur une **architecture des réseaux résiliente** et un **système de défense passive fort**. C'est pourquoi il encourage les différents acteurs à définir des principes régissant l'architecture de ces réseaux ainsi qu'à renforcer les systèmes de défense existant. L'Institut insiste également sur la recherche et le développement de technologies permettant d'assurer un niveau maximal de sécurité. Enfin, il est rappelé que seule une coopération accrue entre l'industrie et les autorités nationales permettront d'atteindre ces objectifs.

[2] AIAA, *The connectivity challenge : protecting critical assets in a networked world. A framework for aviation cybersecurity*, août 2013, p.7, disponible sur http://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf

Dragon Lady, ou l'industrialisation de la cybercriminalité[3]

A l'occasion de la DEF CON 21, la société Lookout a présenté son travail d'enquête sur l'industrialisation des virus sur mobile en Russie. Baptisée « Dragon Lady »[4], cette opération témoigne de la grande organisation de ces réseaux, au point que 60% des virus observés par Lookout soient générés par un noyau d'une dizaine d'entreprises russes, de véritables grossistes du malware SMS. Leur source de revenu : l'arnaque aux SMS surtaxés. Son fonctionnement est simple : forcer un utilisateur à envoyer involontairement un SMS surtaxé, générant des revenus cumulés de plusieurs milliers de dollars.

La particularité de ces réseaux réside dans leur **division du travail**. Ils se divisent les charges et se spécialisent dans un chaînon de l'activité. Une entreprise se charge de l'élaboration des logiciels malveillants, en proposant plusieurs modèles et une large palette de personnalisation pour coller à des applications déjà existantes (Skype, Adobe, Google Play, jeux). Ces logiciels malveillants sont fournis à des intermédiaires affiliés, qui se chargent de les customiser et de les mettre en ligne, par divers canaux de distribution. La consultation de ces liens frauduleux par un utilisateur entraîne l'exécution du malware, qui provoque l'envoi d'un SMS surtaxé rémunérant l'entreprise grossiste et l'intermédiaire affilié. Les profits évoqués sont de l'ordre de dizaines de milliers de dollars mensuels.

Une dizaine d'entreprises grossistes (« Malware HQ ») ont été identifiées, desquelles émaneraient jusqu'à 60% des malwares observés par Lookout. Leur activité se limite à la conception, mais elles n'hésitent pas à démarcher les intermédiaires à l'aide de sites attractifs, proposant leurs services mais également mettant en compétition les intermédiaires. Des classements par montants générés et des récompenses sont proposés, des newsletters et des blogs sont même tenus pour informer les intermédiaires de nouvelles mises à jour, fonctionnalités ou actualités.

Elles proposent des applications Android personnalisables, construites selon les demandes de l'intermédiaire, pour générer des SMS surtaxés venant approvisionner les comptes de l'intermédiaire. Un guide étape par étape est même fourni, conseillant sur la charte visuelle à utiliser (Skype, Adobe, Google Play, jeux, MP3 ou pornographie), détaillant les diverses configurations possibles, et expliquant comment assurer le suivi de la campagne.

[3] Pour approfondir le sujet :

- https://www.lookout.com/resources/reports/dragon-lady
- http://securitywatch.pcmag.com/mobile-security/314386-russia-s-massive-android-malware-industry-revealed
- http://www.pcmag.com/image_popup/0,1740,iid=387084,00.asp
- http://www.zdnet.fr/actualites/en-russie-lookout-pointe-l-emergence-des-startups-du-malware-par-sms-39792926.htm
- http://pro.clubic.com/it-business/securite-et-donnees/actualite-576518-rapport-lookout-malware-industrie.html
- http://tempsreel.nouvelobs.com/societe/20130802.OBS2027/derriere-les-virus-pour-smartphone-10-start-up-mafieuses.html

[4] https://www.lookout.com/resources/reports/dragon-lady

Figure 2. Le cycle de vie d'une campagne (traduction du Nouvel Observateur)[5] :

Les intermédiaires affiliés peuvent dépenser entre 1 000 et 2 000 dollars sur trois mois pour ensuite gérer la campagne et la distribution du malware, pour des revenus de l'ordre de 12 000$. La distribution du malware se fait d'abord par l'insertion du code dans une page web à la charge de l'intermédiaire, dont le lien est propagé par divers canaux, Twitter en tête. Il suffit qu'un utilisateur y accède pour qu'un SMS soit frauduleusement généré. Le profil type des victimes correspond à quelqu'un parlant russe, à la recherche d'application populaires comme Skype, de pornographie ou de fichiers multimédia. Quiconque ne consulte pas le site depuis un terminal mobile ou depuis un pays ciblé est filtré et éconduit. Grossistes et intermédiaires développent des méthodes élaborées d'évitement des anti-virus et opérateurs réseaux, à commencer par Lookout. Obfuscation, chiffrement et filtrage sont mobilisés pour répondre à cet objectif d'évitement.

Une véritable chaîne industrielle du secteur de la fraude au SMS surtaxé s'est développée autour d'une dizaine d'entreprises russes, de l'élaboration au suivi, en passant par la personnalisation, la distribution et la dissimulation. Chaque segment d'activité est encadré, divisé et guidé pour optimiser cette activité, dont l'organisation permet d'accroître les gains. Lookout, par l'opération Dragon Lady, témoigne de l'industrialisation de la cybercriminalité russe.

[5] http://tempsreel.nouvelobs.com/societe/20130802.OBS2027/derriere-les-virus-pour-smartphone-10-start-up-mafieuses.html

iGuardian : la nouvelle arme du FBI dans la lutte contre la cybercriminalité

Début août 2013 le FBI dévoilait son nouveau portail, iGuardian, offrant la possibilité aux entreprises de rapporter les cyberattaques dont elles ont été victimes ou les failles en matière de cybersécurité ayant été découvertes. Ce programme pilote est ouvert aux seules entreprises et institutions membres du réseau **InfraGard** créé par le FBI en 1996 et dont l'objectif est le partage d'informations et d'expertise en matière de cybercriminalité[6]. Avant son lancement, les membres d'InfraGard disposaient d'une multitude de façons de rapporter les cyberattaques. iGuardian permet désormais, non seulement une centralisation de l'information envoyée directement au FBI, mais également de s'assurer que pour chaque rapport les mêmes indications seront transmises, ce qui facilitera l'analyse des données communiquées. Une fois le rapport rempli, les informations révélées sont traitées par le National Cyber Investigative Joint Taskforce (NCI-JTF) qui regroupe 19 agences travaillant sur les questions de cybersécurité.

L'échange d'informations est unilatéral, pour l'instant. Seuls les membres d'InfraGard en transmettent, le FBI n'en fournissant aucune. Cependant, cela pourrait évoluer pour intégrer une analyse des malwares produite par le FBI. Le portail pourrait également être ouvert à des entreprises non-membres du réseau InfraGard[7]. Le vice-directeur du département de la criminalité et des réponses cyber a également annoncé que le FBI travaillait sur le partage d'adresses IP et d'autres indicateurs d'attaques ainsi que sur la mise à dispositions d'agents spécialisés[8].

Les objectifs de ce programme sont multiples. D'une part, il s'agit de détecter où sont les nouvelles cybermenaces et, d'autre part, de permettre au FBI d'enquêter et aux autres entreprises de prendre les mesures adéquates pour se protéger, sans que le nom de l'entreprise victime soit pour autant divulgué et qu'il soit porté atteinte à la réputation de celle-ci.

Le secteur privé a favorablement accueilli cette nouvelle plateforme. Ainsi, Peter CASSIDY, Secrétaire général du Groupe de travail anti-phishing a déclaré que cette base de *données « participait à la fondation d'un modèle de réponse unifié contre la cybercriminalité »*[9]. Mais ce programme n'est pas totalement nouveau. En effet, il s'agit d'une extension du programme e-Guardian, lui-même créé dans le prolongement de Guardian. e-Guardian, créé en 2009, est un portail qui permet aux autorités fédérales et locales de partager des informations liées à la lutte contre le terrorisme.

Le lancement de ce nouveau portail s'inscrit dans les évolutions récentes qui ont marqué la coopération entre le secteur public et le secteur privé dans la lutte contre la cybercriminalité.

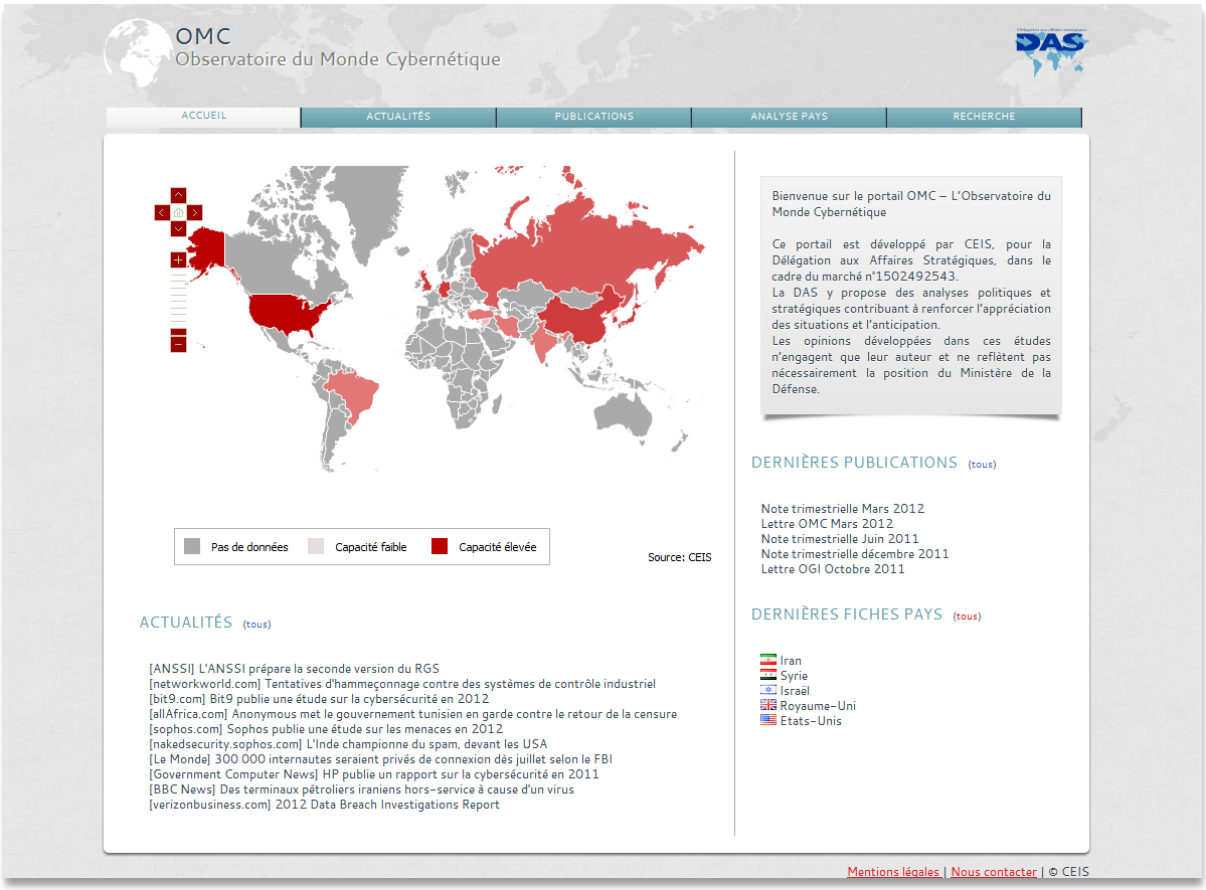
[6] https://www.infragard.org/FsafFT%2525252BDEUrq3EOQ9lsoJSt5VO98yZFD0ua36j7dev8%2525253D!

[7] John P. MELLO Jr., "FBI's new iGuardian portal aims to ease cyber crime reporting", *CSO*, 5 août 2013, disponible sur http://www.csoonline.com/article/737669/fbi-s-new-iguardian-portal-aims-to-ease-cyber-crime-reporting

[8] Amber CORRIN, "FBI launches cyber threat info-sharing platform", *FCW*, 30 juillet 2013, disponible sur http://fcw.com/articles/2013/07/30/fbi-information-sharing.aspx

[9] John P. MELLO Jr., "FBI's new iGuardian portal aims to ease cyber crime reporting", *op. cit.*

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



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

Sommet Ground Zero	New Delhi, Inde	7-10 septembre
Cyber Security for National Security (CS4NS)	Charleston, Etats-Unis	10 septembre
At&T Cyber Security Conference	New York City, Etats-Unis	10 septembre
Petit-déjeuner de l'Observatoire du FIC	Paris	11 septembre
GS Mag : Le Data Center de demain	Paris	17 septembre
Cyber Intelligence Europe	Bruxelles	17 – 19 septembre
Hackaton Open Data des Alpes-Maritimes	Sophia Antipolis	20-21 septembre
Trophées de la Sécurité	Paris	23 septembre
Cyber Security for the Chemical/Petrochem Industry	Texas, Etats-Unis	24 - 25 septembre
Mois de la Cybersécurité	Europe	Octobre
Petit-déjeuner européen du FIC / Mois de la cybersécurité (EN)	Bruxelles, Belgique	15 octobre
Cyber Security Summit	Minneapolis, Etats-Unis	22-23 octobre
ICS Cyber Security Conference	Atlanta, Etats-Unis	21-24 octobre
API Cybersecurity Conference & Expo	Houston, Etats-Unis	12-13 novembre

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