Observatoire du Monde Cybernétique

Lettre n°34 – Octobre 2014

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

Actualités p. 2

- 2èmes Rencontres parlementaires de la cybersécurité : les partenariats public/privé au cœur des débats.
- DEFNET 2014 : premier exercice global de cyberdéfense français.
- La DGA au cœur de la cyberdéfense française.
- Arrivée de 200 militaires spécialistes de la cyberdéfense au camp de la Maltière en 2015.
- Lancement d'Antibot.fr, pour promouvoir la lutte contre les botnets.
- Moscou et Pékin sur le point de signer un accord sur la cybersécurité.
- La Conférence de plénipotentiaires de l'UIT élit Houlin Zhao comme nouveau Secrétaire général.
- Comment définir l'acte d'agression dans le cyberespace ?
- Sandworm team : une campagne de cyberespionnage attribuée à la Russie ?
- L'opération Pawn Storm.
- APT28 : au cœur des opérations de cyberespionnage russes ?
- Opération SMN : analyse de l'unité de hackers d'élite Axiom.
- Le SOCOM veut se lancer dans le data-mining avec AVATAR.
- Le projet TOR identifie un nœud malicieux en Russie.
- Ukraine : la commission électorale victime d'une attaque informatique la veille des législatives.
- Israël crée une nouvelle autorité chargée de la cyberdéfense.
- Couper Internet, la solution russe en cas de conflit ?
- A Hong Kong, les iPhones des manifestants pour la démocratie ont été touchés par un virus.
- Renforcement de la coopération de cyberdéfense entre Israël et l'Inde.

Analyse des menaces p. 5

Cybercriminalité et guerre de l'information : la montée en puissance des cartels mexicains

A l'heure où la cyberdélinquance ne cesse d'augmenter au Mexique, classé 3ème pays d'Amérique latine en termes de cybercriminalité, les cartels ont investi Internet avec une réelle dextérité. Outil d'espionnage, de menaces en ligne ou de guerre de l'information, le Web est désormais un enjeu stratégique pour les cartels mexicains, comme en témoigne leur récent conflit avec Anonymous.

Agenda p. 10

2èmes Rencontres parlementaires de la cybersécurité : les partenariats public/privé au cœur des débats

A 10 mois de la Loi de Programmation Militaire, les intervenants de la première table-ronde ont dressé un bilan des actions menées. Parmi les initiatives listées, les travaux de l'ANSSI menés en collaboration directe avec les OIV constitue un bon exemple de coordination public/privé. [GSM] Le débat suivant sur le partenariat public/privé animé par Laure de la Raudière, député d'Eure et Loir, a démontré l'importance de renforcer les échanges afin de renforcer la cyberdéfense. [GSM]

[defense.gouv.fr] DEFNET 2014 : premier exercice global de cyberdéfense français

Le ministre de la Défense, Jean-Yves Le Drian, s'est rendu du 30 septembre au 3 octobre 2014, aux écoles de Saint-Cyr Coëtquidan (ESCC) afin d'assister à l'exercice interarmées DEFNET 2014. Mobilisant une soixantaine de participants, il s'agit du premier exercice interarmées de cyberdéfense simulant une attaque des systèmes informatiques. L'exercice DEFNET avait pour objectif d'entraîner les forces spécialisées du niveau le plus bas jusqu'au niveau du commandement des opérations.

Les missions reposent sur la gestion de crise ou encore le déploiement de groupe d'intervention rapide (GIR). DEFNET 2014 sera reconduit pour une nouvelle édition en mars 2015.

[Métropole Rennes] La DGA au cœur de la cyberdéfense française

Avec 250 experts dans ce domaine, la mission de la DGA consiste, entre autres, à sécuriser les systèmes d'information et les systèmes d'armes des forces françaises. Avec la construction d'un nouveau bâtiment de 10 000 m2 sur son site, pour lequel le ministre de la Défense, Jean-Yves Le Drian, a posé la première pierre le 7 octobre 2014, la DGA Maîtrise de l'information emploiera en 2017 quatre cents personnes dans le domaine de la cyberdéfense, principalement des ingénieurs.

[OuestFrance] Arrivée de 200 militaires spécialistes de la cyberdéfense au camp de la Maltière en 2015

Le ministre français de la Défense, Jean-Yves Le Drian a annoncé le déploiement de 200 militaires spécialistes de la cyberdéfense sur la base militaire de la Maltière à Saint-Jacques-de-la-Lande. La majorité de ces 200 militaires sera affectée dans une nouvelle compagnie de combat cyber électronique (108 personnes en 2019) et dans une antenne du Calid (centre d'analyse en lutte informatique défensive, 75 personnes en 2019).

De plus, un renfort de 400 personnes a été annoncé d'ici 2017 à la DGA-MI de Bruz (ex-Celar).

[Antibot] Lancement d'Antibot.fr

C'est le 12 octobre que le site de lutte contre les botnets, Antibot.fr, a été lancé. Soutenu par le CeCyf et la Gendarmerie nationale, le site se veut être le point central d'information européen sur la lutte contre les botnets. Le projet s'inscrit dans le cadre de l'Advanced Cyber Defence Centre. Objectifs : partager l'information, aider à la détection et au nettoyage des ordinateurs.

[kommersant.ru] Moscou et Pékin sur le point de signer un accord sur la cybersécurité

Moscou et Pékin seraient sur le point de conclure un accord historique en matière de cybersécurité. Ce *deal* favorisera le lancement d'opérations et de projets communs en matière de « sécurité de l'information ». Le traité pourrait également prévoir une *hotline* entre les deux pays, activable en cas de crise.

[GSM] La Conférence de plénipotentiaires de l'UIT élit Houlin Zhao comme nouveau Secrétaire général

A l'issue du vote ayant eu lieu au cours de la séance plénière de la Conférence de plénipotentiaires de 2014, c'est le chinois Houlin Zhao, seul candidat en lice, qui a été élu Secrétaire général de l'UIT. Il entrera en fonction le 1er janvier 2015 pour une durée de 4 ans.

[Stefano Mele] Définir l'acte d'agression dans le cyberespace

Dans cette étude, l'auteur se lance dans un exercice de définition de ce qu'est un acte de guerre dans le cyberespace, à l'aide de critères d'évaluation. Il propose également une série de recommandations à l'égard des décideurs du secteur public et du secteur privé afin d'améliorer leur compréhension du sujet.

[iSight] Sandworm team : une campagne de cyberespionnage attribuée à la Russie ?

iSight lève le voile sur une opération de cyberespionnage massive ayant ciblé des acteurs des secteurs militaire, de la Défense, et des ONG : OTAN, gouvernent ukrainien, gouvernement polonais, des entités académiques américaines, voire quelques entreprises européennes du secteur des télécommunications... Cette campagne remontant à 2009 serait le fait de l'équipe de pirates informatiques baptisée Sandworm par iSight partners (préalablement surnommée « Quedach » par F-Secure). Mais contrairement à F-Secure, iSight prétend aller plus loin en présentant plus de données, et en démontrant notamment l'usage de la faille zero-day CVE-2014-4114. iSight attribue cette campagne d'espionnage à la Russie, son agenda et ses différentes étapes et cibles répondant aux intérêts géopolitiques du pays. Sandworm team aurait notamment ciblé des acteurs français du secteur des télécommunications via une variante du malware BlackEnergy précédemment repéré par F-Secure [F-Secure] en juin dernier. Notons que les travaux de recherche ont été menés en partenariat avec Microsoft.

[Trend Micro] L'opération Pawn Storm

Le 22 octobre, Trend Micro dévoilait l'opération de cyberespionnage baptisée « Pawn Storm ». Cette campagne, menée par des acteurs actifs depuis 2007, aurait ciblé divers acteurs du monde militaire, économique, des gouvernements et des médias, mais aussi des opposants et dissidents politiques russes. Trois vecteurs d'attaque ont été exploités. Le premier : du spear phishing présentant un document infecté par SEDNIT/Sofacy en pièce-jointe ; le second : des sites web de phishing assortis de typosquatting, ciblant principalement les utilisateurs de l'application Web d'Outlook (OWA) ; le troisième, la compromission de sites légitimes par iframes malicieuses, afin de disséminer le malware SEDNIT/Sofacy.

[FireEye] APT28 : au cœur des opérations de cyberespionnage russes ?

Dans son dernier rapport, FireEye décrypte le mode opératoire du groupe de hackers surnommé APT28. L'opération de cyberespionnage aurait ciblé des acteurs de la Défense américains, des organisations européennes et des entités gouvernementales d'Europe de l'est, mais aussi des manifestations publiques européennes telles qu'EuroNaval 2014 ou Eurosatory 2014. FireEye présente dans son document un faisceau d'indices désignant la Russie comme instigateur. APT28 aurait privilégié le spear phishing comme vecteur d'attaque. On y retrouverait également Sofacy, malware exploité dans le cadre de l'opération Pawn Storm dévoilée par Trend Micro.

[Novetta] Opération SMN : analyse de l'unité d'élite Axiom

C'est au cours de l'opération de nettoyage « SMN » qu'une coalition de chercheurs en sécurité informatique a découvert l'unité de hackers informatique Axiom. Ce groupe composé de hackers d'« élite » disposerait de ressources conséquentes lui permettant de cibler des acteurs gouvernementaux aux Etats-Unis et en Europe. L'unité, qui se concentre sur le cyberespionnage industriel et de dissidents politiques, agirait pour le compte de la Chine.

Novetta, société de cybersécurité, est à la tête de cette coalition qui regroupe aujourd'hui des acteurs tels que Microsoft, Tenable, FireEye, Cisco, F-Secure, Threat Connect ou Symantec.

[TorProject] Le projet TOR identifie un nœud malicieux en Russie

TOR a identifié que l'un de ses nœud de sortie était utilisé afin d'infecter les terminaux des utilisateurs, notamment lorsque ceux-ci procédaient à des téléchargements de fichiers. Le nœud a été blacklisté, et ne sera plus utilisé.

TOR fonctionne sur un système de chiffrement « en onion », grâce à plusieurs nœuds de connexion ; le nœud de sortie de connexion est généralement considéré comme le plus vulnérable.

[dhnet.be] Ukraine : la commission électorale victime d'une attaque informatique la veille des législatives

La commission électorale ukrainienne a été visée, à la veille des législatives, par une attaque DDoS rendant inaccessible temporairement le site www.cvk.gov. Répondant aux affirmations de l'agence de presse russe Ria-Novosti, les équipes informatiques du gouvernement ont rapidement rassuré sur Facebook : l'attaque n'aurait pas eu d'impact sur le scrutin, et aurait même été anticipée, notamment dans un contexte de crise donnant lieu à une multiplication des cyberattaques à l'encontre des infrastructures ukrainiennes.

[RFI] Israël crée une nouvelle autorité chargée de la cyberdéfense

L'Etat israélien a annoncé la création d'une nouvelle autorité chargée de la cyberdéfense du pays ; en parallèle, il souhaite également renforcer les partenariats public/privé. Cette autorité de cyberdéfense centralisera une grande partie des capacités de défensives et offensives de l'Etat.

[La Tribune] Couper Internet, la solution russe en cas de conflit ?

Un quotidien local rapporte que la Russie prévoit de se doter d'un « segment russe de l'internet » utilisable en « situations d'urgence », au regard de « l'imprévisibilité totale des États-Unis et de l'Union européenne ». Objectif : se doter des outils nécessaires pour réagir dans le cas où la Russie se retrouverait « coupée de l'internet mondial ». En marge de ces discussions, est également prévu le renforcement de la sécurité des infrastructures du pays.

[South China Morning Post] A Hong Kong, les iPhones des manifestants pour la démocratie ont été touchés par un virus

Des chercheurs en cybersécurité ont identifié un nouveau malware touchant les produits Apple (*jailbreakés*) des manifestants pour la démocratie à Hong Kong. Ce virus, connu sous le nom de Xsser, est capable de voler des messages, des photos, ou encore les mots de passe sur les iPhones et les iPad. Selon le directeur de l'entreprise américaine Lacoon Mobile Security, Michael Shaulov, le virus Xsser est le malware le plus sophistiqué utilisé à ce jour contre les utilisateurs iOS.

[IsraelValley] Renforcement de la coopération de cyberdéfense entre Israël et l'Inde

Le 28 septembre 2014, à l'occasion de l'Assemblée générale des Nations Unies, le Premier ministre israélien, Benjamin Netanyahu, a rencontré son homologue indien, Narendra Modi. Les deux ministres ont discuté du renforcement de la coopération de cyberdéfense, dans les domaines civil et militaire.

Cybercriminalité et guerre de l'information : la montée en puissance des cartels mexicains

Le 16 octobre 2014 à Tamaulipas, une activiste mexicaine qui dénonçait les crimes commis par les cartels est retrouvée morte. Elle participait de façon anonyme à un réseau de journalistes citoyens dans l'état de Tamaulipas[1]**.** La photo de son cadavre est « exhibée » sur son propre compte Twitter[2]. Le compte de la victime, Maria del Rosario Fuentes Rubio, avait été piraté quelques semaines plus tôt, laissant apparaître des messages funestes. Pour les Mexicains, cet assassinat vient s'ajouter à la longue litanie des meurtres qui endeuillent le pays quotidiennement. En octobre 2013, la DEA recensait plus de 80 000 morts liées directement au narcotrafic depuis 2005[3]. Profitant des largesses d'une police corrompue et d'un système bancaire complice, les cartels mexicains sont des véritables multinationales criminelles. Leurs domaines d'activité comprennent également le racket, les enlèvements, mais également des vols exponentiels d'hydrocarbures[4]. Toutes ces activités enracinent l'assise régionale de certains cartels[5]. A l'heure où la cyberdélinquance ne cesse d'augmenter au Mexique, classé 3ème pays d'Amérique latine en termes de cybercriminalité[6], les cartels ont investi Internet avec une réelle dextérité.

La conquête du Web : un enjeu stratégique pour les cartels mexicains

Dans un pays où presque 3 milliards de dollars[7] ont été volé via internet en 2013, le marché de la cybercriminalité est devenu un enjeu stratégique pour les cartels de drogue. Leur présence sur internet s'articule autour de plusieurs activités allant d'une stratégie de « soft power », de promotion de la « culture narco », de cybercriminalité mais aussi de menaces à l'encontre d'internautes un peu trop curieux.

Le vol de données sensibles

Les cartels ciblent les banques, les entreprises pétrolières ou encore certaines personnalités politiques, l'objectif final étant principalement la recherche de bénéfices. Par exemple, des informaticiens travaillant pour le compte des cartels ont pu obtenir des informations concernant les employés de l'entreprise pétrolière PEMEX. Ils ont ainsi pu les soudoyer pour savoir comment voler du pétrole des gazoducs[8].

Le cyberespionnage

[1] « Les assassins d'une journaliste mexicaine twittent sa mort », publié le 22/10/2014 in *L'Express,* dipsonible à l'adresse suivante http://www.lexpress.fr/actualite/monde/amerique-sud/les-assassins-d-une-journaliste-mexicaine-twittent-sa-mort_1614486.html

[2] « Narcos matan a tuitera y cuelgan la foto en su propia cuenta », publié le 16/10/14 in *El Comercio*, disponible à l'adresse suivante http://elcomercio.pe/mundo/latinoamerica/narcos-matan-tuitera-y-cuelgan-foto-su-propia-cuenta-noticia-1764498

[3] « En 8 años, la guerra contra las drogas de México acumula mas muertos que 10 años de guerra en Vietnam », publié le 21/10/2013 in *Sin embargo*, disponible à l'adresse suivante http://www.sinembargo.mx/21-10-2013/788369

[4] « Narco-finance, les impunis », documentaire de 88 minutes, *Arte Thema*, disponible à l'adresse suivante http://www.parismatch.com/Actu/International/La-blogueuse-mexicaine-qui-fait-trembler-les-cartels-508535

[5] BENITEZ MANAUT Raul., *Altas de la Sécurité y de la Défense du Mexique 2009*, Colectivo de Análisis de la Seguridad con Democracia (CASEDE). Disponible à l'adresse suivant http://www.seguridadcondemocracia.org/

[6] «Mexico, tercer lugar en ciberdelincuencia en América latina : UNAM », publié le 22/09/14 in *Estado Mayor*, disponible à l'adresse suivante http://estadomayor.mx/47012

[7] « Mexico, tercer lugar en ciberdelincuencia en América latina : UNAM », publié le 22/09/14 in *Estado Mayor*, disponible à l'adresse suivante http://estadomayor.mx/47012

[8] « Carteles roban millones en petroleo, publié le 25/09/14, in *Tele Mundo* disponible à l'adresse suivante http://www.telemundolasvegas.com/mexico/Carteles-roban-millones-en-petroleo-pemex-mexico-narcotrafico-277068961.html

Les barons de la drogue sont régulièrement au courant des opérations tactiques de l'armée mexicaine, si bien qu'ils peuvent se préparer contre d'éventuelles opérations commandos. Enfin, grâce aux nouvelles technologies comme le GPS, les cartels multiplient les kidnappings[9].

La promotion de la « narco culture » via les réseaux sociaux

Une véritable stratégie de communication en ligne permet aux narcotrafiquants de recruter de nouveaux membres, de maîtriser leur image et de consolider leur pouvoir. Les narcotrafiquants font leur promotion en s'affichant par exemple dans des véhicules imposants, brandissant des fusils d'assaut. D'autre plus « people » postent des vidéos vantant les avantages d'être un « narco ». Ainsi, le *leader* du cartel Los Caballeros Templarios a posté une vidéo de 30 minutes sur Youtube, à visage découvert, qui comptabilise déjà plus d'un million de vues[10].

Les cybermenaces à l'adresse des internautes

A travers leurs blogs, les cartels donnent des avertissements et des messages aux internautes qui menaceraient de divulguer des informations sensibles, comme en témoigne la photo de Rosario Fuentes Rubio postée sur son propre profil Twitter.

La maitrise du Web par les cartels de drogue ne serait pas effective sans l'enlèvement d'experts en informatique pour surveiller les activités des cartels concurrents, les commentaires des réseaux sociaux à leur encontre ou encore éviter qu'ils ne soient la cible d'une prochaine cyberattaque[11]. En 2012, 36 ingénieurs ont ainsi été enlevés. Néanmoins nombreux sont les informaticiens à rejoindre d'eux-mêmes les cartels de drogue. En offrant 70 000 euros pour deux jours de travail[12], le crime organisé sait en effet se rendre attractif et compétitif, dans un pays touché par l'extrême pauvreté.

Mobilisation des internautes contre les cartels de drogue

[9] « Les cartels de la drogue s'emparent du web », publié le 16/01/14 in *JDD*, disponible à l'adresse suivante http://www.lejdd.fr/International/Ameriques/Les-Cartels-de-la-drogue-s-emparent-du-web-648784

[10] « Les cartels de la drogue s'emparent du web », publié le 16/01/14 in *JDD*, disponible à l'adresse suivante http://www.lejdd.fr/International/Ameriques/Les-Cartels-de-la-drogue-s-emparent-du-web-648784

[11] PEDROSA DE ABREU José, « Mexican Drug Cartels and Cyberspace : Oppotunity and threat », publié le 21/03/2012 in *Infosec Institute*, disponible à l'adresse suivante http://resources.infosecinstitute.com/mexican-cartels/

[12] « Narco-finance, les impunis », documentaire de 88 minutes, *Arte Thema*, disponible à l'adresse suivante http://www.parismatch.com/Actu/International/La-blogueuse-mexicaine-qui-fait-trembler-les-cartels-508535

[12] « Réseaux sociaux contre cartels de drogue », publié le 10/11/2011 in *Courrier International*, disponible à

Face à l'impuissance de la police, corrompue par les barons de la drogue, les mexicains se sont mobilisés. Les internautes recensent les activités des narcotrafiquants, comme le blog emblématique Del Narco, fermé depuis mai 2014, suite à la disparition d'un des deux contributeurs. Le groupe Anonymous au Mexique est aussi très impliqué dans la lutte contre les narcotrafiquants et leurs partenaires[13]. A titre d'exemple, le site internet de l'ancien procureur de Tabasco, Gustavo Rosario Torres, avait été piraté et on pouvait lire sur la page d'accueil : « Gustavo Rosario est un Zeta », du nom de l'une des organisations criminelles les plus violentes du pays. Les hackers ont revendiqué cette cyberattaque en postant une vidéo sur YouTube[14].

En septembre 2011, les Zetas, composée d'anciens policiers et de militaires d'élite, décidaient de contre-attaquer en exécutant des internautes. Le 26 septembre 2011, la journaliste Marisol Macías Castañeda était retrouvée décapitée pour avoir divulgué des données sensibles mettant en cause des policiers et des narcotrafiquants sur son blog et son compte Twitter[15]. Toujours en septembre 2011, la police de Nuevo Laredo avait retrouvé, pendus sous un pont, les cadavres mutilés de deux blogueurs avec un premier message de menaces à l'encontre des internautes mexicains, lui aussi signé des Zetas[16]. Le 6 octobre 2011, un internaute du groupe Anonymous postait une vidéo dans laquelle il annonçait qu'un membre du collectif avait été enlevé par les cartels des Zetas alors qu'il participait à l'Opération Paperstorm, une distribution de tracts appelant à rejoindre le monde libre d'Anonymous[17]. Les *leaders* du groupe ripostèrent immédiatement en annonçant qu'ils allaient divulguer les noms des narcotrafiquants et pirater leurs comptes bancaires. Un combat frontal baptisé #OpCartel. L'un des leaders du groupe, Barrett Brown, affirmait qu'ils avaient réussi à pirater 25 000 mails contenant des informations sur 75 complices des Zetas[18].

Mais le 1er novembre 2011, l'entreprise américaine Stratfor, spécialisée dans le renseignement et le contre-terrorisme, affirmait que les Zetas auraient massivement recruté des hackers pour pirater les Anonymous et dévoiler à leur tour leur identité. Cette information entraîna un arrêt temporaire de la campagne de lutte contre le cartel de Los Zetas. L'opération reprit le lendemain avec la déclaration de Barrett Brown, de

[13] REXTON KAN Paul, « Cyberwar in the underworld : Anonumous versus Los Zetas in Mexico », 2012, in *Yale Journal of international Affairs*, 12 pages
[14] « Réseaux sociaux contre cartels de drogue », publié le 10/11/2011 in *Courrier International*, disponible à l'adresse suivante http://www.courrierinternational.com/article/2011/11/10/reseaux-sociaux-contre-cartels-de-la-drogue?page=all
[15] WAGSTAFF Keith, « Fourth Blogger reportdly killed by Los Zetas Mexican Durg Cartel », publié le 10/11/2011 in *Time*, disponible à l'adresse suivante http://techland.time.com/2011/11/10/fourth-blogger-reportedly-killed-by-los-zetas-mexican-drug-cartel/
[16] RILEY Michael, « Mexico's drug war takes to the blogosphere », publié le 09/11/2011 in *Bloomber Businessweek*, disponible à l'adresse suivante http://www.businessweek.com/magazine/mexicos-drug-war-takes-to-the-blogosphere-11092011.html
[17] « Réseaux sociaux contre cartels de drogue », publié le 10/11/2011 in *Courrier International*, disponible à l'adresse suivante http://www.courrierinternational.com/article/2011/11/10/reseaux-sociaux-contre-cartels-de-la-drogue?page=all
[18] CHEN Adrian, « Spokesman says Anonymous will use 25,000 stolen emails to expose Mexican drug cartel », publié le 11/03/2011 in *Kinja*, disponible à l'adresse suivante http://gawker.com/5856138/spokesman-says-anonymous-will-use-25000-stolen-emails-to-expose-mexican-drug-cartel

réactiver l'opération #OpCartel. Face à la pression des Anonymous et la peur de voir leurs identités révélées, les narcotrafiquants libèrent l'otage le 4 novembre 2011[19]. Les Anonymous ont ainsi souhaité faire une démonstration de puissance, montrer leur capacité à affronter cet autre pouvoir qu'est le narcotrafic.

Conclusion

Omniprésent sur le net, les cartels se servent des réseaux sociaux comme d'une vitrine pour afficher leurs activités criminelles mais aussi le luxe qui en découle. Les menaces qu'ils adressent aux internautes conduisent parfois à des assassinats. La multiplication de ces meurtres apporte une nouvelle dimension au crime organisé : le narco-terrorisme mexicain transposé en ligne s'est désormais doté d'un volet numérique stratégique.

Cette omniprésence pourrait néanmoins déboucher sur une dépendance accrue des cartels à Internet. Leurs opposants l'ont bien compris et luttent aussi en ligne notamment en dénonçant les membres des cartels via le réseau anonymisant TOR. En 2011, la libération d'un des membres du groupe Anonymous marque une étape décisive dans l'évolution des conflits numériques opposant les cartels aux internautes.

[19] « Mexique : des Anonymous entrent en guerre contre un cartel », publié le 04/11/2011 in *Le Nouvel Observateur*, disponible à l'adresse suivante,
http://tempsreel.nouvelobs.com/vu-sur-le-web/20111104.OBS3851/mexique-des-anonymous-entrent-en-guerre-contre-un-cartel.html

Le portail OMC
La plateforme de la DAS

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

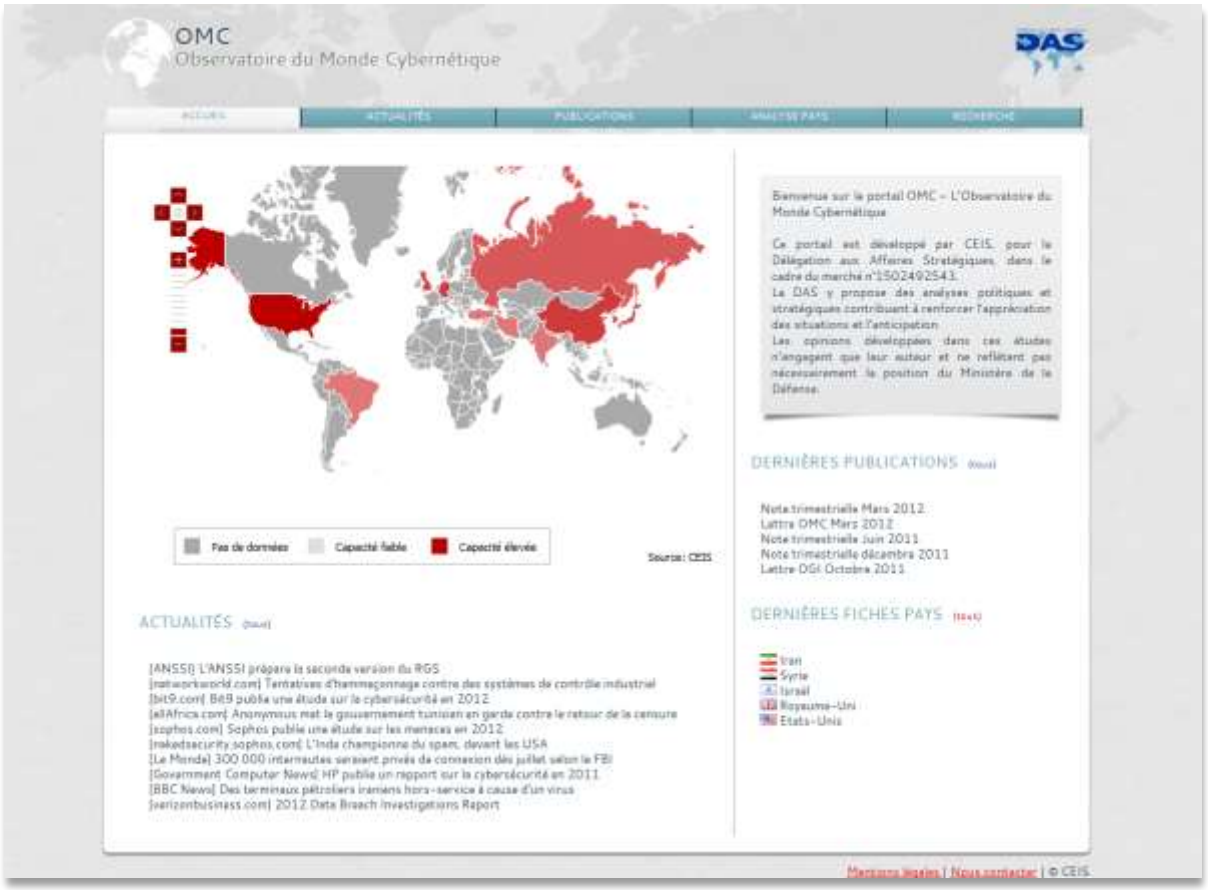

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

OpenStack Summit Paris	Paris	3 - 7 novembre
5th Annual Open Source Digital Forensics Conference (OSDFCon)	Herndon, VA, Etats-Unis	5 novembre
Security Pressures: What Really Matters	Manchester, Royaume-Uni	6 novembre
Cyber Security Awareness Week	Brooklyn, NY, Etats-Unis	13 – 15 novembre
Cyber Security Forum & Expo	Robins Air Force base	18 novembre
IT Expo	Paris	18 – 19 novembre
No Such Con	Paris	19 – 21 novembre
Montpellier : DigiWorld Summit 2014	Montpellier	18 – 20 novembre
Cyber Security SUMMIT 2014	Londres	20 novembre
6th IRISSCERT Cyber Crime Conference	Dublin	20 novembre
Cyber Security World Conference 2014	New York City, Etats-Unis	21 novembre
DefCamp	Bucharest, Roumanie	25 – 29 novembre
Botconf	Nancy	3 – 5 décembre

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