Observatoire du Monde Cybernétique

Lettre n°31 – Juillet 2014

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

[Legifrance] Le décret n° 2014-845 offrira plus d'autonomie au directeur de l'ANSSI

Le décret n° 2014-845, pris par le Premier ministre et paru le 30 juillet au Journal Officiel, dispose que le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pourra dorénavant signer, au nom du Premier ministre et par délégation, les actes relevant du champ de compétences de l'agence. Ce décret offre ainsi une plus grande autonomie à l'ANSSI et devrait encore améliorer sa réactivité.

[Ouest France] Un pôle pour développer la cyberdéfense en Bretagne

La Bretagne et l'Institut national de recherche en informatique et automatique (Inria), basé à Rennes, vont signer une convention de trois ans pour « développer la recherche et la formation dans le domaine de la cybersécurité ». Ce partenariat s'appuiera sur la présence : du centre d'expertise DGA Maîtrise de l'information à Bruz, des centres de formation de l'École des transmissions (ETRS) et des écoles de Saint-Cyr Coëtquidan, ainsi que sur un tissu académique et industriel dense.

[The Guardian] Le représentant des services secrets américains expulsé d'Allemagne

Le gouvernement allemand a intimé au représentant des services secrets américains pour l'Allemagne de quitter le pays. Cette expulsion est une conséquence directe de l'affaire d'espionnage de responsables allemands révélée par Edward Snowden. Clemens Binninger, membre du comité parlementaire aux affaires d'espionnage et d'intelligence a justifié cette expulsion en affirmant que les services secrets américains n'ont apporté aucune réponse aux questions des autorités allemandes sur cette affaire d'espionnage.

[Le Figaro] Espionnage : l'Allemagne envisage le retour à la machine à écrire

Afin de contrer les méthodes d'espionnage de la NSA, les huit députés chargés d'enquêter sur l'étendue des écoutes de la NSA en Allemagne, utiliseraient une machine à écrire. Cette méthode est également utilisée par les services spéciaux russes à la suite des révélations d'Edward Snowden. D'autres précautions ont également été mise en place par la commission d'enquête. Par exemple, avant chaque réunion, les participants doivent déposer téléphones et ordinateurs dans une boîte métallique afin d'éviter toute communication avec l'extérieur.

[lavenir.net] Belgique : le gouvernement finalise l'arrêté royal sur la création d'un centre pour la cybersécurité

Le gouvernement fédéral a finalisé l'arrêté royal qui doit permettre la création d'un centre belge pour la cybersécurité. Le « Centre Cyber Security Belgique » sera placé sous l'autorité du Premier ministre.

Il aura un rôle de coordination entre les différents services de l'État (Sûreté de l'État, Service de renseignement militaire, Centre de crise, Computer Crime Unit) et un rôle opérationnel. En effet, il sera responsable de la gestion de crise en cas de cyberincidents ; il forgera une stratégie de cybersécurité pour le pays ; et il sera en charge de l'élaboration et de la diffusion « des standards, directives et normes de sécurité pour les différents types de système informatique des administrations et organismes publics ». Le Centre disposera d'un effectif d'une dizaine de personnes.

[The Telegraph] Royaume-Uni : un budget de 800 millions de livres sterling débloqué

Dans une tribune écrite pour le Telegraph, le 14 juillet, David Cameron (Premier ministre du Royaume-Uni) a affirmé qu'il considérait la cyberdéfense comme l'un des trois éléments essentiels à la stratégie de défense du pays (avec le développement de la technologie aéronautique et l'augmentation des moyens mis à disposition des forces spéciales). En conséquence, un budget de 800 millions de livres sterling sera alloué au développement des technologies de cyberdéfense.

[Zdnet] L'OTAN met à jour sa politique de cyberdéfense

Considérant la place croissante de la dimension cyber au sein des conflits internationaux, l'OTAN a mis à jour sa politique de cyberdéfense. Désormais, une cyberattaque peut être considérée comme équivalente à une attaque conventionnelle, et donc potentiellement sujette à l'article 5 de la clause de défense collective (une attaque contre l'un des membres de l'OTAN « sera considérée comme une attaque contre tous les membres »).

Cette nouvelle direction sera ratifiée lors du sommet de Wales en septembre 2014.

[France 24] Al-Qaïda – EIIL : guerre de communication entre frères ennemis

L'État islamique en Irak et au Levant et le Front Al-Nosra (branche d'Al-Qaïda en Syrie) se sont lancés dans une guerre de communication et d'images sur le web en *« s'attaquant à coups de hashtags, de tweets »* et de photos. Ainsi, le Front Al-Nosra, qui signifie le « Front de la Victoire » est devenu le « Front de la perte et de la traîtrise » et des photos mettant en scène le cadavre de l'un des chefs du Front (barbe rasée et couvert de billets) ont été postées sur twitter.

[Numerama] Israël : Netanyahu achète des tweets publicitaires contre le Hamas

Depuis le lancement de l'opération militaire israélienne « Bordure Protectrice », les cyber militants pro-palestiniens et pro-israéliens ont inondé les sites de réseaux sociaux (Facebook, Twitter) de photos du conflit.

Selon le journal « Aujourd'hui », une guerre de ''Hashtag'' a donc lieu entre #GazaUnderAttack et #IsraelUnderFire. Le bureau du Premier Ministre d'Israël aurait ainsi versé une certaine somme d'argent à Twitter afin que l'un de ses messages condamnant le Hamas soit affiché en tant que « tweet sponsorisé », lui assurant ainsi plus de visibilité.

[Bloomberg] En 2010, le NASDAQ a été infecté par un malware capable de causer des dommages critiques à son système de gestion du marché d'action

Bloomberg a dévoilé, mercredi 17 juillet, l'existence d'une cyberattaque qui aurait pu plonger dans le chaos l'ensemble du système financier américain. La complexité du mode opératoire d'infection du système (utilisation de deux vulnérabilités zero-day, complexité du malware) indiquait que seule une agence de renseignement ou une unité militaire pouvait être à l'origine d'une telle attaque. Les agences de renseignement américaines (NSA, CIA) et le FBI ont attribué, non-officiellement, cette cyberattaque à la Russie.

[The Guardian] E. Snowden conseille aux professionnels détenant des informations sensibles de les chiffrer

Au cours d'une interview accordée au Guardian, Edward Snowden a affirmé qu'au vu des capacités d'espionnage de la NSA, il était du devoir des avocats, journalistes et médecins de chiffrer les informations sensibles qu'ils détiennent sur leurs sources et leurs clients.

[The Intercept] Nouvelles révélations de Greenwald et Snowden : le GCHQ disposerait de logiciels capables de manipuler l'opinion sur le Web

Glenn Greenwald a révélé, lundi 14 juillet, que le GCHQ a développé une série d'outils lui permettant de récupérer des informations sur des internautes, notamment des photos privées postées sur Facebook (SPRING BISHOP), de manipuler les résultats de sondages en lignes (UNDEPASS), d'augmenter artificiellement le nombre de vues d'une page Web (SLIPSTREAM), de censurer des vidéos en lignes jugées extrémistes (SILVERLORD), d'activer Skype sur un ordinateur afin d'enregistrer des conversations, d'analyser la liste des contacts et d'envoyer des messages à ces contacts (MINIATURE HERO), de surveiller l'activité d'utilisateurs du site eBay (ELATE), de connecter

deux téléphones sur un même appel (IMPERIAL BARGE), de lancer des cyberattaques de type DDoS (PREDATORS FACE), d'amplifier le nombre de vues et de « like » d'une vidéo postée sur Youtube (GESTATOR) et d'usurper l'identité électronique d'un utilisateur d'Internet (CHANGELING).

[Google] Google annonce le lancement de "Project Zero" ciblant les vulnérabilités "zero-day"

Google a annoncé, mardi 15 juillet, la création de « Project Zero ». Ce projet réunit une équipe d'hackers d'élite et d'experts en cybersécurité dont le but sera de protéger les utilisateurs de Google Chrome, Gmail et Internet Explorer contre des cyberattaques exploitant les vulnérabilités « zero-day », telles que « heartbleed ».

[Security Week] Le FBI et le DOJ demandent plus de moyens pour lutter contre les Botnets

Au cours d'une audition devant la Commission Parlementaire sur les Activités Criminelles et Terroristes, des représentants du FBI et de l'US Department of Justice ont demandé au Congrès de voter une loi leur donnant plus d'outils et de moyens pour combattre les opérateurs de Botnets. Cette demande est soutenue par Microsoft, Symantec, Farsight Security et Online Trust Alliance. Selon l'avocat de l'Unité de Lutte contre la Criminalité Numérique de Microsoft, 500 millions d'ordinateurs seraient infectés par des Botnets, causant une perte financière de 9 milliards de dollars pour les États-Unis et de 110 milliards de dollars pour la planète.

[Threatpost] Facebook et la Division Cyber Crime grecque démantèlent le Botnet Lecpetex

Dans une opération conjointe, Facebook et la Division du Cyber Crime grecque ont pris le contrôle du Botnet Lecpetex le 3 juillet 2014, Botnet qui avait infecté 250 000 ordinateurs. Le malware associé au Botnet avait deux objectifs principaux : voler les identifiants des utilisateurs (Facebook, mais aussi banques en ligne et Paypal) et utiliser la puissance de calcul des ordinateurs infectés pour miner des litecoins.

[SYMANTEC] Plus de 1000 entreprises du secteur de l'énergie aux États-Unis et en Europe touchées par Dragonfly

Symantec a dévoilé, mardi 1 juin, que plus de 1000 entreprises du secteur de l'énergie aux États-Unis et en Europe ont été compromises par des cyberattaques lancées, depuis 2013, par le groupe de hackers Dragonfly. Les pays européens concernés sont l'Espagne, la France, l'Italie, la Turquie et la Pologne.

[Army Times] Lancement d'une formation cyber pour les commandants de l'Armée de Terre

L'USCYBERCOM a lancé une formation cyber afin de donner, aux commandants de l'Armée de Terre qui seront déployés au sol, une meilleure compréhension des capacités de support et des dommages que les unités cyber peuvent potentiellement infliger. Cette formation permettra d'améliorer la complémentarité et l'interaction entre les unités cyber et les officiers de l'Armée de Terre dirigeant les opérations au sol. La 1st Information Opérations Command mènera donc des exercices Red Team – Blue Team dans les centres de formations des officiers de l'Armée de Terre.

[ITAR-TASS] La cybersécurité : pierre angulaire de la coopération russo-brésilienne ?

À la veille de son périple diplomatique en Amérique Latine (Brésil, Argentine et Cuba), Vladimir Poutine a donné une interview à l'agence de presse ITAR-TASS au cours de laquelle il a mis en avant les principaux points de discussions qui seront abordés avec la chef d'État brésilienne Dilma Rousseff. Selon le chef d'État russe, l'un des principaux domaines de coopération entre ces deux pays sera la cybersécurité et la lutte contre le cyberespionnage.

Il s'est ainsi joint au point de vue de Dilma Rousseff, exposé au cours de la 68ème Assemblée Générale de l'ONU, en affirmant que « le cyberespionnage est une violation directe de la souveraineté d'un État » et que les deux pays coopéreront dans le développement d'un

« système international de sécurité des systèmes d'informations ».

[ECNS] La Chine annonce l'ouverture du « People's Liberation Army Cyberspace Strategic Intelligence Research Center »

Le gouvernement chinois a annoncé, lundi 30 juin, l'ouverture d'un centre de recherche militaire de cyber intelligence appelé « People's Liberation Army Cyberspace Strategic Intelligence Research Center ». Ce centre sera rattaché au General Armaments Department et aura comme mission de rechercher de nouveaux outils et de nouvelles stratégies de renseignement et de collecte d'informations.

[abc.net] L'effectif cyber de l'Armée nord-coréenne aurait doublé en l'espace de deux ans

Selon une source militaire contactée par l'agence de presse sud-coréenne « Yonhap », l'effectif cyber de l'Armée nord-coréenne aurait doublé en l'espace de deux ans, passant ainsi de 3000 en 2012 à 5900 en 2014. De plus, cette source affirme qu'une unité attachée au General Bureau of Reconnaissance, et composée de 1200 hackers, serait installée en Chine d'où elle lancerait des cyberattaques contre la Corée du Sud.

[RIA Novosti] La Russie reprend son centre d'interception à Cuba

Selon le quotidien russe Kommersant, la Russie et Cuba ont convenu de remettre à la disposition de la Russie le centre de guerre électronique de Lourdes, près de La Havane. Cette base, fermée en 2001, est le seul complexe russe de renseignement d'origine électromagnétique situé dans l'hémisphère occidental.

[Periscope Daily Defense News Capsules] La Collective Security Treaty Organization a initié la création d'un Centre de cyberdéfense

La Collective Security Treaty Organization (CSTO), regroupant l'Arménie, la Biélorussie, le Kazakhstan, le Tadjikistan et la Russie, a initié la création d'un centre de cyberdéfense. Selon le secrétaire général de la CSTO, Khaibullo Latypov, le projet est encore dans sa phase embryonnaire.

[NDTV] Narendra Modi, Premier ministre indien, affirme qu'il est du devoir des BRICS de préserver l'espace numérique comme un bien commun mondial

Narendra Modi, Premier ministre indien, a affirmé lors de son discours devant les chefs d'États des BRICS (Fortaleza, 14 juillet 2014) qu'il était de leur devoir de préserver l'espace numérique comme un bien commun mondial. Enfin, il a affirmé l'importance de la coopération entre les conseillers en matière de sécurité nationale (National Security Advisors) des BRICS au vue de l'émergence des enjeux de cybersécurité.

[Globes] Le gouvernement israélien offre des allègements fiscaux aux entreprises décidant de s'établir au parc national cybernétique de Beersheva

Afin de dynamiser l'activité du parc national cybernétique de Beersheva, le gouvernement israélien a approuvé une loi offrant des allègements fiscaux aux entreprises qui décideraient de s'y établir. Benjamin Netanyahu a affirmé que cette décision répond à un besoin stratégique de l'État, « le secteur cyber s'affirmant comme un élément essentiel de la défense nationale ».

L'opération Bordure Protectrice sous l'angle cyber

Le conflit israélo-palestinien s'est transposé depuis plusieurs années dans le cyberespace. Au-delà des affrontements entre les forces cyber de l'armée israélienne, celles du Hamas et du Hezbollah, des hacktivistes ont conduit des attaques répétées contre Israël. Si les effets de ces campagnes de cyberattaques sont à relativiser, elles ont néanmoins un effet mobilisateur.

Alors que l'opération Bordure Protectrice[1], qui fait l'objet d'un intense traitement médiatique, soulève l'indignation d'une partie de l'opinion publique, on constate un affrontement d'une rare intensité entre groupes de hackers. Cette intensité tranche avec la discrétion d'acteurs cyber aux capacités plus sophistiquées et aux objectifs politiques plus marqués. Pourtant, cette discrétion ne signifie pas « inaction ». Les actions des hacktivistes et hackers patriotes peuvent au contraire offrir des opportunités stratégiques, et peuvent être liées des actions menées par des attaquants de plus haut niveau.

Il semble que l'opération Bordure Protectrice entraîne donc logiquement un conflit cyber à deux vitesses. Ce conflit est cependant original du fait de la virulence des acteurs visibles, qui peuvent ouvrir des opportunités pour d'autres acteurs.

Un affrontement virulent sur le devant de la scène

Une forte mobilisation pro-palestinienne

« Ceci est un appel urgent à tous les hackers, organisations de défense des droits de l'homme, activistes à travers le monde : ce soir, unissons-nous pour commencer une campagne contre Israël, pour montrer ce qui se passe réellement [...] Rejoignez le cyber-intifada le 11 juillet. Opération Save Gaza engagée »

Les opposants à Israël se rassemblent autour de deux opérations. La première, #OpIsrael[2], existe depuis 2012 et a donné lieu à plusieurs campagnes de cyberattaques initiées par Anonymous. La seconde, *#OpSaveGaza*[3], a été créée le 3 juillet 2014 par Anon Ghost Team en réaction à l'opération militaire israélienne à Gaza. Elle a rassemblé un grand nombre de groupes de hackers pour une vague de cyberattaques contre plus de 2000 sites Internet israéliens le 11 juillet 2014. Parmi les groupes de hackers ayant suivi *#OpSaveGaza* se trouvent *Izzah Hackers*, la *Tunisan Hackers Team*, the *Indonesian Cyber Army*, the *Middle East Cyber Army (MECA)*, *Anonymous Arab* et la *Muslim Liberation Army*[4].

[1] http://tsahal.fr/tag/operation-bordure-protectrice/

[2] http://rt.com/news/anonymous-israel-cyber-attack-737/

[3] https://www.youtube.com/watch?v=iyQA3zMg7ZQ&list=UUJ7eFTLJArvkgDBae1hbllw

[4] http://www.geektime.com/2014/07/20/israeli-hackers-launch-a-proportionate-response-to-hamas-cyber-intifada/

L'objectif de ces attaquants est de « punir » Israël pour son attaque à Gaza, par le biais de cyberattaques visant à compromettre la sécurité des acteurs civils ou militaires israéliens, en diffusant des contenus pro-palestiniens, ainsi qu'en pénalisant économiquement Israël. Dans cette optique, la nature des attaques varie entre les dénis de service distribué (DDos), les défacements de site Internet israéliens ou pro-israéliens, et les fuites de données.

Deux éléments peuvent être constatés. Tout d'abord, ces vagues d'attaque ont frappé un éventail extrêmement large d'acteurs civils israéliens, allant des petits commerces à la grande distribution ou même les banques. D'autres attaques de plus haut niveau ont été menées contre des cibles militaires ou stratégiques. La *Tunisian Hackers Team* a ainsi annoncé avoir transmis à des « mouvements de résistance palestiniens » des données récupérées sur des ordinateurs de l'armée israélienne. La *Middle East Cyber Army (MECA)* a également revendiqué plusieurs actions, parmi lesquelles une attaque réussie contre le système téléphonique israélien.

Les hackers pro-palestiniens ont donc lancé des cyberattaques contre un large éventail de cibles afin de punir la société israélienne dans son ensemble, exprimer leur solidarité avec les palestiniens, voire donner un avantage aux mouvements de résistance en transmettant les données stratégiques récupérées. Cependant, aucune attaque n'a été reportée contre les infrastructures critiques israéliennes.

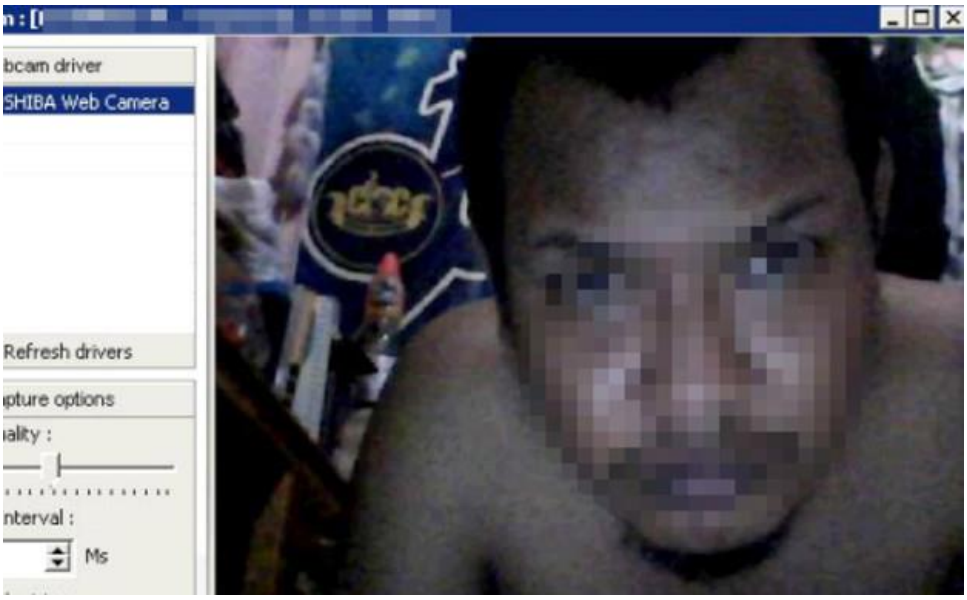
Une réponse originale des pro-israéliens

Hey, next time do not take part in an offensive against Israel. We know who you are, we know where you are. Praise Israel.

Face à la mobilisation des hackers pro-palestiniens, un groupe de hackers pro-israélien, *l'Israeli Elite Force (IEF)*, a lancé un contre-attaque intitulée #OpIsraelRetaliate. L'IEF a appelé les hackers soutenant Israël à attaquer les sites pro-palestiniens, à diffuser des contenus pro-israéliens, et à révéler l'identité des hackers adverses. Créée en avril 2013[5] en prévision de l'opération #OpIsrael du 5 avril 2013, *l'Israeli Elite Force* (IEF)

[5] http://www.thedailybeast.com/articles/2013/04/08/why-opisrael-was-an-opfail.html

n'en est pas à son coup d'essai. Elle apparaît surtout comme le produit des campagnes de cyberattaques qu'Israël subit à un rythme régulier. Ainsi, si l'attaque de sites Internet pro-palestiniens n'a rien de surprenant, le fait de rechercher et de révéler l'identité de ces hackers est relativement nouveau. Alors que les groupes de hackers anti-israéliens planifiaient l'attaque #OpIsraelBirthday en avril 2014, l'IEF a lancé l'opération #OpBirthControl dans le but de repérer les attaquants, diffuser leur identité[6] et ainsi tenter de les dissuader d'agir. Ce mode d'action a eu un fort impact médiatique et est à nouveau utilisé dans le cadre de #OpIsraelRetaliate. Les membres de l'IEF ont ainsi publié les données personnelles et les photos prises par webcam de nombreux hackers pro-palestiniens.



Un bruit de fond et beaucoup de données

Les cyberattaques effectuées dans le cadre des opérations #OpIsrael, #OpSaveGaza et #OpIsraelRetaliate ont pour point commun un niveau de sophistication relativement faible, ainsi que le fait d'être dirigé contre un large éventail de cibles. En plus de médiatiser leurs succès, les hackers des deux camps annoncent transmettre les données recueillies aux combattants des deux camps. Ces données ainsi que le « bruit de fond » créé par les nombreuses attaques peuvent représenter une opportunité pour d'autres types d'attaquants.

Une opportunité pour d'autres acteurs

Si les actions des groupes de hackers pro-palestiniens ou pro-israéliens ont une forte visibilité, elles ne constituent que des attaques « en surface », ne causant pas de dommages importants. Elles peuvent cependant ouvrir la voie pour des attaques beaucoup plus élaborées et potentiellement plus destructrices.

Un « bruit de fond» élevé

Les attaques répétées des différents groupes de hackers pro-palestiniens nécessitent une mobilisation des équipes de cyberdéfense israéliennes. Elles peuvent susciter chez les défenseurs une habituation aux

[6] https://twitter.com/th3j35t3r/status/453747969825964032

attaques, ou une saturation pouvant réduire leur niveau d'attention. Des cyberattaques plus sophistiquées et plus furtives auraient donc potentiellement plus de chances de réussir dans ce contexte.

Des informations sensibles révélées

Les annonces des groupes de hackers peuvent constituer du renseignement d'intérêt cyber sur l'identité des défenseurs, ou sur les vulnérabilités des différentes installations. Les attaques systématiques contre un large éventail d'installations révèlent au quotidien les vulnérabilités de nombreuses entreprises ou installations israéliennes qui peuvent être exploitées plus avant par d'autres groupes. Côté israélien, la publication par l'IEF des identités des attaquants qui transfèrent potentiellement des données aux mouvements pro-palestiniens peut leur permettre d'établir une surveillance et de repérer des cibles ayant un intérêt militaire.

Vers une évolution des opportunistes ?

La virulence des attaques entre groupes de hackers constitue donc un terreau fertile pour des attaques de plus haut niveau. Au-delà de la volonté de punir et de dissuader les deux camps, les attaquants préparent le terrain pour des acteurs qui ne sont pas encore rentrés dans le conflit, ou qui peuvent saisir l'opportunité de mener des opérations de cyberespionnage moins susceptibles d'être détectées dans le « bruit de fond » ambiant.

A travers ce prisme, il est ainsi possible de s'interroger sur l'intérêt d'Israël à voir apparaître des informations vieilles de deux ans sur un vol de technologies concernant l'Iron Dome[7], ou sur la non-implication de groupes de hackers potentiellement soutenus par des Etats dans le conflit. Sous cet angle, la discrétion de la Syrian Electronic Army (SEA) pourtant virulente contre Israël[8], et à même de mener des opérations de sabotage, est particulièrement intéressante[9].

[7] http://hackread.com/chinese-hackers-israel-iron-dome-data/

[8] http://legalinsurrection.com/2014/07/syrian-electronic-army-hijacks-israel-defense-forces-twitter-account/

[9] http://www.globalpost.com/dispatch/news/regions/middle-east/130525/syrias-electronic-army-attempted-attack-haifas-water-system

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

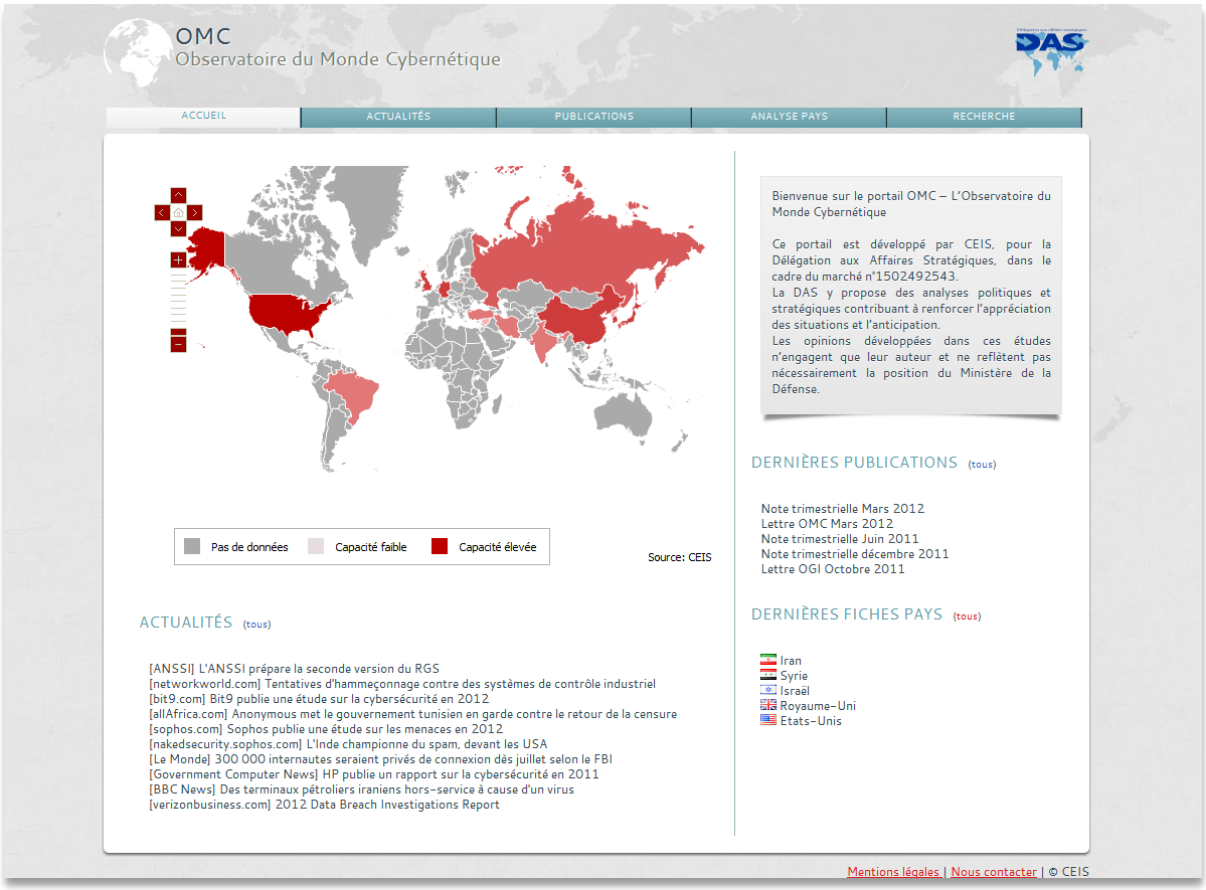


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Black Hat USA	Las Vegas	2 - 7 août
SecProTec East Africa 2014	Kenya	20 - 22 août
Cyber Europe 2014	Belgique	22 - 24 septembre
NFC World Congress	Marseille	22 - 24 septembre
Les Assises de la Sécurité	Monaco	1 - 4 octobre
Black Hat Briefings & Training Europe	Amsterdam	14 - 17 octobre

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