Observatoire du Monde Cybernétique

Lettre n°32 – Août 2014

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

[Legifrance] Nouveau décret relatif au système d'information et de communication de l'Etat.

Un décret datant du 1er août 2014 dispose que le système d'information de l'Etat est désormais placé sous la responsabilité du Premier ministre. La responsabilité de ce décret est, de plus, délégué de plein droit aux ministres dans la mesure requise pour l'exercice de leurs attributions. La responsabilité des points suivants n'est pas déléguée à une entité administrative autre que le Premier ministre, sauf décision de sa part :

1° Infrastructures informatiques ;
2° Réseaux de communication ;
3° Services numériques d'usage partagé ;
4° Systèmes d'informations relatifs à des fonctions transversales des administrations de l'Etat.

[ANSSI] Le Premier ministre français lance sa première Politique globale SSI.

La PSSIE a été instaurée par le biais d'une circulaire du Premier Ministre, le 17 juillet 2014. Cette politique fixe les règles de protection applicables aux systèmes d'information de l'Etat. Dix principes fondamentaux sont initiés dans cette politique, permettant à l'Etat et aux organes administratifs de concevoir leurs infrastructures réseaux, dont les produits sont certifiés par l'ANSSI. L'entrée en vigueur de cette politique est immédiate. Elle servira de modèle méthodologique aux institutions souhaitant développer un document de la même nature.

[The Hacker News] Le téléphone d'Hillary Clinton intercepté par les services de renseignements allemands.

Après les allégations d'écoutes de la chancelière Allemande Angela Merkel par la NSA et la CIA, la Bundesnachrichtendienst (BND), le service de renseignements allemand, aurait intercepté au moins une communication issue du téléphone d'Hillary Clinton, durant son service en tant que Secrétaire d'Etat.

Les services allemands ont toutefois nié avoir eu recours à ces tentatives d'espionnage et ont indiqué que les écoutes ont été obtenues accidentellement. D'autres sources journalistiques allemandes font état que les services ont conservé ces enregistrements, sans les détruire après leur réception. Cette annonce est moins surprenante du fait que l'Allemagne a mis en place un large système informatisé de contre-espionnage pour se protéger de ses partenaires occidentaux et pouvoir agir à son tour dans le cyberespace.

[Le Monde] L'Ukraine et la Russie au bord de la cyberguerre.

Un virus, dénommé « Snake », a infiltré les ordinateurs du bureau du Premier ministre ukrainien et d'une dizaine d'ambassadeurs ukrainiens en Europe. Selon un rapport de Symantec, publié le 7 août 2014, des informations sensibles auraient été dérobées. L'auteur de ce virus serait la Russie, car le code source du virus contient des mots russes. Cependant rien d'autre ne permet d'affirmer avec certitude la provenance du virus. Les experts de BAE Systems annoncent que le virus s'est propagé rapidement depuis 1 an sur les réseaux ukrainiens, malgré une implantation du virus effective depuis 2006 dans toute l'Europe.

[Bloomberg] La Banque Centrale Européenne victime d'une extorsion de fonds.

Après avoir attaqué les systèmes informatiques de la Banque Centrale Européenne, un groupe non encore identifié de pirates a pris contact avec les membres de l'organisation pour obtenir une rançon. Les pirates ont menacé de dévoiler des informations sur les conférences et les présentations internes de la BCE. Aucune donnée personnelle n'était en jeu et les dirigeants de la BCE ont rapidement fait appel à la police allemande.

[Kasperky Lab] L'Opération "Epic Turla" expliquée

Dans son dernier rapport du 7 août 2014, Kaspersky Lab dévoile une campagne de cyberespionnage qui a sévi en Europe. Durant près de 10 mois, les équipes de Kaspersky ont analysé les tendances de l'opération qu'ils ont baptisé

« Epic Turla ». L'objectif des pirates était de pouvoir infiltrer les réseaux des ambassades, d'entreprises privées, des services de santé, les services militaires et les réseaux gouvernementaux.

Ce sont donc près de 20 pays qui ont été touchés par cette campagne, principalement situés en Europe et au Moyen-Orient. Les auteurs infiltraient les sites internet jugés essentiels et profitaient de cette opportunité pour infecter les visiteurs et les personnels qui s'y connectaient.

[Mashable] Des hackers russes annoncent avoir dérobés plus de 1,2 milliards identifiants et mots de passe.

Hold Security, une société de sécurité informatique, à découvert récemment une faille sur internet qui aurait permis de dérober plus de 1.2 milliards identifiants et mots de passe, ainsi que 500 millions d'emails.

Après 18 mois de recherches et d'enquête, les experts ont découvert que des pirates russes auraient dérobé ces informations, grâce à l'utilisation de botnets et de failles sur des sites internet. L'opération aurait été initiée en 2011, par une douzaine de jeunes russes âgés d'une vingtaine d'années.

[Daily Dot] La Russie fait un pas de plus vers la censure.

Le groupe informatique Russia League for Internet Safety, propose un nouveau système pour filtrer les contenus sur internet. Le contenu d'un site est analysé et filtré en temps réel, selon deux niveaux, et peut être immédiatement blacklisté. Le système de censure est testé depuis plusieurs mois et vient d'être approuvé par la dernière législation du pays sur la censure de contenus adultes sur internet.

[SecureList] Les experts de Kaspersky ont découvert un malware espagnol utilisé en Amérique Latine.

Le malware Machete est un outil de cyberespionnage espagnol lancé en 2010 et amélioré en 2012. Encore actif, le malware propose des outils de surveillance, tels qu'un keylogger, l'enregistrement audio via les microphones, la géolocalisation des ordinateurs et la copie de fichiers sur un serveur externe. Les victimes de ce malware sont hispanophones et sont localement situées au Vénézuela, en Eqauteur et en Colombie. Le malware a également été découvert dans de nombreux systèmes en Europe, Asie et Amérique Latine.

[The Washington Post] Les entreprises américaines assistent l'industrie du spyware outre-Atlantique.

La société CloudShield Technologies a pris part au développement d'outils de surveillance de masse, vendus par Gamma International, une société britannique spécialisée dans ce domaine. Le Washington Post et l'Université de Toronto ont enquêté sur ces allégations pour prouver le rôle des compagnies américaines dans l'élaboration de logiciels type spyware vendus dans le monde. La législation américaine est très stricte sur les principes de coopération dans ce domaine, et cette révélation peut nuire au développement de CloudShield Technologies sur les marchés occidentaux. Les sociétés contactées nient toute implication dans la conception de ce genre de logiciel.

[MatthewAid] Les capacités de cybersécurité augmentent sensiblement pour l'US Cyber Command.

L'Amiral Mike Rogers, à la tête du US Cyber Command et de la NSA, a annoncé l'augmentation importante des capacités du Cyber Command en matière de cybersécurité pour les Etats Unis. Une plus grande collaboration sera effective et un renforcement des capacités en ressources humaines sont à prévoir.

[The Wall Street Journal] Une importante cyberattaque touche la société USIS aux Etats-Unis.

Au début du mois d'août, le gouvernement américain annonçait la suspension de son

partenariat avec l'USIS, fournisseur de solutions de sécurité, alors victime d'une cyberattaque.

Des informations sur les employés du Department of Homeland Security auraient été dérobées grâce à cette attaque, qui n'est pas revendiquée et dont le gouvernement ne peut affirmer l'origine. Le FBI tente d'identifier les auteurs de ce délit, et les 240,000 employées du DHS doivent avertir de tout problème financier sur leurs comptes bancaires.

[Jerusalem Post] L'Iran aurait initié de nombreuses attaques informatiques sur Israël.

Selon un expert en sécurité qui souhaite conserver l'anonymat, l'Iran aurait, durant le conflit entre Israël et le Hamas, tenté de pirater les systèmes de communications civils de l'Etat hébreu. D'autres tentatives d'intrusion ont été lancées contre les forces de l'IDF en opérations dans la bande de Gaza, mais l'Iran n'aurait pas atteint ses objectifs.

[Arbor Networks] Analyse des attaques DDoS dans le contexte du conflit entre Israël et le Hamas.

Dans son dernier rapport sur l'analyse des attaques DDoS contre Israël, Arbor Network définit une tendance générale à la hausse des attaques depuis le début du conflit conventionnel entre Israël et les forces du Hamas. L'étude démontre une quantité plus importante et une durée toujours plus longue des attaques DDoS contre Israël, malgré les décisions diplomatiques et les actes unilatéraux en faveur d'une baisse des tensions dans la région.

[IISS] La cyberguerre et les rapports conflictuels entre Etats-Unis et Chine.

Avec une hausse des tensions dans la région de l'Asie-Pacifique, une situation de quasi-Guerre froide est instaurée entre la Chine et les Etats-Unis, les experts se demandent donc quel acteur s'engagerait à démarrer les hostilités en premier sur le cyberespace. Le potentiel et les capacités en matière de cybersécurité des deux pays ne sont pas à démontrer, mais les experts s'accordent à dire que la situation est sans précédent. Les tensions portent à la fois sur des aspects conventionnels et relevant du cyberespace, pouvant mener à des offensives multiples sur les deux niveaux. Le rapport des experts apporte quelques clés quant à la possible réduction des tensions dans cette région du globe.

[Defense News] La Chine lance plusieurs cyberattaques contre Taïwan.

Le 13 août dernier, le ministère des Sciences et des Technologies taïwanais annonçait être la victime d'attaques informatiques chinoises. Les unités de cyberdéfense chinoises et taïwanaises s'affrontent chaque jour depuis plusieurs mois, le but étant pour la Chine de récupérer des informations jugées sensibles par le gouvernement de Taïwan. La Chine profite de ses capacités technologiques et en ressources humaines pour mener des attaques massives contre les infrastructures taïwanaises et les sites internet gouvernementaux.

[Xinhua Net] La Chine veut développer son propre système d'exploitation.

Dès le mois d'octobre 2014, l'industrie logicielle de Chine devrait proposer une première version d'un nouveau système d'exploitation, pour remplacer Windows, Android ou iOS sur les terminaux de l'Etat. Ce projet est issu d'une alliance entre plusieurs industriels et universitaires, dont Ni Guangnan est à la tête. Objectif : développer un OS afin de soutenir une certaine souveraineté numérique.

[South China Morning Post] Des sociétés Hongkongaises victimes d'une cyberattaque globale.

Quatre des plus importants fournisseurs d'accès internet hongkongais ont subi une attaque majeure sur leurs infrastructures le 10 août dernier. Les pirates à l'origine de Synolocker ont initié cette attaque. Ils ont utilisé les failles matérielles du constructeur taïwanais Synology, qui fournit la majorité des appareils des compagnies hongkongaises. Les sociétés craignent que désormais les appareils mobiles des utilisateurs soient infectés ; ceux-ci doivent être

prudents et les faire tester au plus vite, sous peine de propagation ultérieure des malwares.

[The Intercept] Comment la NSA a construit son propre système de recherche semblable à Google : ICREACH

D'après les documents de la NSA dévoilés par Edward Snowden, la création d'ICREACH représente une avancée historique dans la gestion des données de surveillance et l'accès à celles-ci. ICREACH est un moteur de recherche réservé aux membres des services de renseignements. Les données extraites sont des écoutes téléphoniques, des emails et des rapports de surveillances de toutes les agences américaines. Le système ICREACH propose une base de recherche complète et regroupe l'ensemble des bases de données des services de sécurité américains.

[The Guardian] Quatre banques américaines victimes d'une cyberattaque russe.

La banque JP Morgan, et quatre autres sociétés, ont été victimes d'une cyberattaque russe. Les pirates russes auraient dérobé les informations confidentielles de ces établissements bancaires. Les enquêteurs du FBI ont annoncé que les pirates représentaient une vraie menace, car possédant de très bonnes capacités techniques. La coordination de ces attaques et l'objectif permettent au FBI d'annoncer que de simples hackers n'auraient pas pu réaliser ces tentatives.

Réouverture de la base de Lourdes, quels enjeux ?

Lors de la première étape de son voyage officiel en Amérique Latine, le Président Vladimir Poutine aurait donné le 11 juillet 2014[1] son accord pour la réouverture de la base d'écoutes de Lourdes, à proximité de La Havane. Cette annonce s'inscrit dans un contexte général de refroidissement continu des relations entre les Etats-Unis et la Russie.

Considérée comme « l'œil de Moscou », la base d'écoute de Lourdes aurait permis de collecter du renseignement par le biais d'interceptions des communications provenant du territoire américain. Plus importante du genre, elle a rempli de nombreuses fonctions et a connu des évolutions de 1962 à 2001, date de sa fermeture officielle.

Evolution des capacités et objectifs de la base de 1962 à 2001

A sa création en 1962, la base d'écoutes de Lourdes avait pour but de collecter du renseignement à partir d'interceptions de communications émises depuis le territoire américain. Elle a également servi à surveiller les mouvements de l'armée américaine, et à sécuriser des communications avec l'Amérique Latine. En 1991, elle aurait permis à la Russie d'obtenir des informations sur les plans américains avant le déclenchement de l'opération Tempête du Désert.

A la chute de l'URSS, les objectifs de la base ont été modifiés pour également intégrer la collecte de renseignement à des fins économiques. Dans cette optique, la base de Lourdes connut une montée en capacité en 1996, sur ordre du Président Boris Eltsine.

"The strategic significance of the Lourdes facility has grown dramatically since the secret order from Russian Federation President [Boris Yeltsin] of 7 February 1996 demanding that the Russian intelligence community step up the theft of American and other Western economic and trade secrets. It currently represents a very formidable and ominous threat to U.S. national security as well as the American economy and infrastructure."

A l'époque, l'administration Clinton ne semblait pas vouloir s'opposer au fonctionnement de la base et à sa montée en capacité[2].

Yet the Clinton Administration insists that it is in America's interest to allow the GRU to continue its eavesdropping on the U.S. In congressional testimony delivered on March 16, 1995, Assistant Secretary of State for Inter-American Affairs Alexander Watson asserted that pressuring Russia to discontinue sigint activities in Cuba "could limit our ability to promote reform and stability in Russia" as it could "be seen by the Russians as interfering with the exercise of their right under the START Treaty to monitor compliance with the agreement...."

La base fut néanmoins fermée en 2001, dans un contexte de rapprochement de la Russie avec les Etats-Unis, et au motif de coûts d'entretiens trop élevés (annoncés à 200 millions de dollars par an). Entre 1996 et 2001, il est probable que l'espionnage économique et la surveillance régionale soient devenus les activités centrales de la base. Par ailleurs, la proximité géographique a pu perdre de son intérêt sur cette période du fait de la montée en puissance des moyens cybers russes qui ne nécessitent pas ce type d'installation hors du territoire national pour collecter du renseignement.

[1] http://www.courrierinternational.com/article/2014/07/17/une-oreille-bien-placee-pour-la-russie
[2] http://cryptome.org/jya/rusigint.htm

En conclusion, il semble que la fermeture de la base puisse être liée à la fois au développement de capacités cybers qui rendaient la proximité géographique moins nécessaire au renseignement, ainsi qu'à une volonté russe de se rapprocher des Etats-Unis sur la scène internationale. Ainsi, si le refroidissement actuel des relations entre la Russie et les Etats-Unis peut motiver la réouverture de la base de Lourdes sur le plan politique, il convient de se demander quelle pourrait être son utilité concrète.

Utilité de la base de Lourdes en 2014

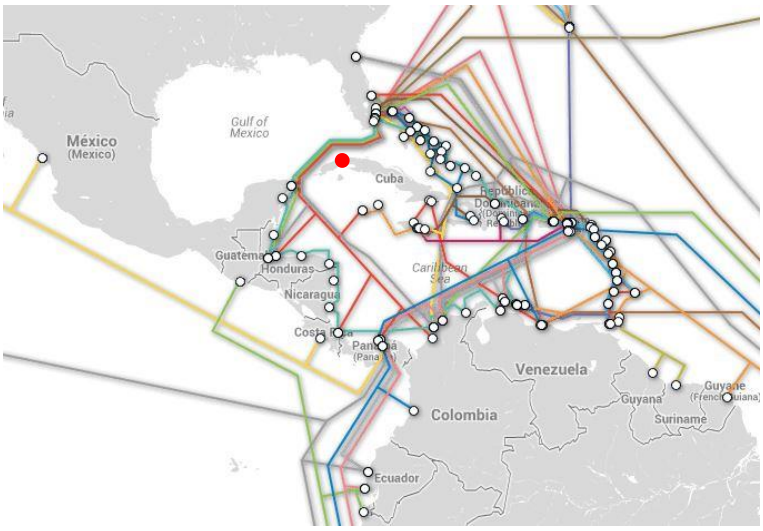
Au-delà de l'intérêt politique de l'annonce, la réouverture de la base de Lourdes devrait permettre à la Russie d'améliorer sa collecte de renseignement dans la région par le biais de plusieurs moyens.

Les interceptions des communications sur le territoire américain.

La base de Lourdes serait en mesure d'intercepter les communications satellitaires sur le territoire américain. Ces capacités étaient déjà développées en 1993, au moment où Lourdes « fournissait 75% des communications américaines captées par Moscou[3] » selon le Ministre de la Défense cubain de l'époque, Raul Castro. Lourdes a d'ailleurs une importance renforcée car la Russie ne disposerait plus de satellites de renseignement capables de mener des interceptions des communications émanant du territoire américain[4]. Au moins deux éléments peuvent cependant limiter l'intérêt des interceptions des communications satellitaires aujourd'hui : le chiffrement systématique des communications militaires américaines, et l'incapacité d'intercepter les communications filaires. L'espionnage économique sur des communications satellitaires non chiffrées peut cependant présenter un intérêt, qui apparaît à lui seul relativement faible par rapport au coût de réouverture de la base.

Un potentiel accès aux câbles sous-marins de la région.

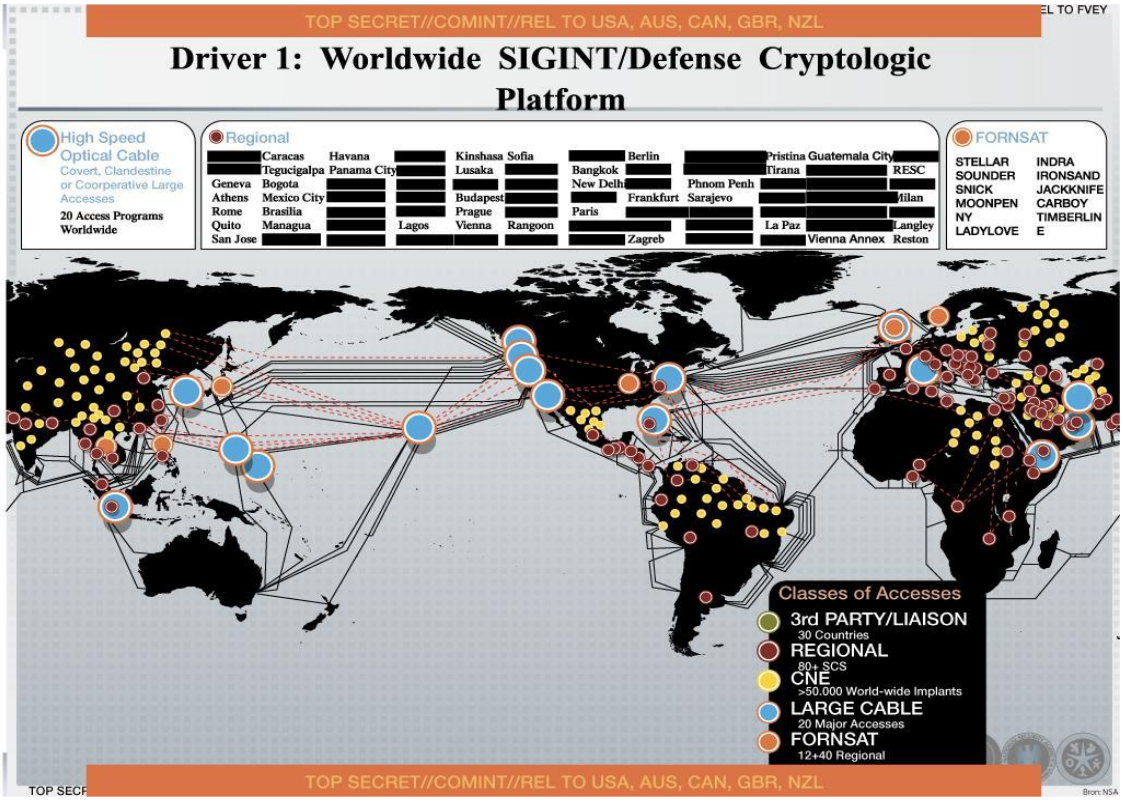
Les câbles sous-marins reliant le continent américain au reste du monde passent en quasi-totalité par le territoire des Etats-Unis. Bien que Cuba n'ai accès qu'au câble ALBA-1, la plupart des câbles reliant l'Amérique du Sud et l'Amérique du Nord passent à proximité. L'île est d'ailleurs située au sud du « nœud » de câbles de Miami.



[3] http://www.courrierinternational.com/article/2014/07/17/une-oreille-bien-placee-pour-la-russie
[4] http://www.laht.com/article.asp?ArticleId=2344132&CategoryId=14510

● Base de Lourdes

Cette position géographique stratégique pourrait permettre à la Russie d'installer des stations de collecte de données qui seraient ensuite traitées directement à Lourdes. Les Etats-Unis possèdent au moins six stations de ce type sur les nœuds de câbles situés sur leurs territoires (en bleu ci-dessous), dont une à proximité de Miami, qui leur permettent de collecter une grande quantité de données en transit selon la méthode « upstream ».



Faire de même à partir de Lourdes, et en « amont » de Miami, pourrait permettre à la Russie de collecter une très grande quantité de données en provenance et à destination d'Amérique Latine. Le traitement de grandes quantités de données que ce type de collecte implique nécessite des moyens importants et de l'énergie, qui pourraient faire partie intégrante de l'accord passé par la Russie avec Cuba. La construction des quatre centrales électriques thermiques pour laquelle la Russie s'est engagée, et qui devrait doubler la production d'électricité de Cuba d'ici 2030[5], pourrait permettre à la base de Lourdes de mener cette mission.

Précéder les stations d'écoutes américaines. En se plaçant en « amont » de la station d'interception située à proximité de Miami, la Russie peut bénéficier à travers Lourdes d'un accès stratégique aux informations transitant sur les câbles en direction des stations américaines. Elle peut également faciliter les communications de la Russie directement avec les pays d'Amérique Latine, comme elle avait pour mission de le faire avant sa fermeture en 2001.

Un « expansionnisme cyber » russe ?

[5] http://www.leparisien.fr/flash-actualite-economie/cuba-entame-la-renovation-de-sa-production-electrique-avec-l-aide-de-moscou-16-07-2014-4005635.php

Politiquement, l'annonce de la réouverture de la base de Lourdes constitue un signal fort pour les représentants des pays d'Amérique Latine et des BRICS que Vladimir Poutine a rencontrés lors de son voyage officiel. Cette initiative pourrait apparaître légitime à leurs yeux car elle illustre la perte de confiance envers les Etats-Unis, et montre l'importance des pays d'Amérique Latine pour la Russie. Quand les BRICS s'accordent pour la construction d'un câble sous-marin visant à éviter le territoire américain, la Russie se positionne en amont des stations américaines.

Il semble possible que la base de Lourdes soit en partie utilisée pour collecter des données sur les câbles de la région. L'intérêt décroissant des interceptions de communications satellitaires sur le territoire américain, et le développement de capacités de cyberespionnage rendent d'autant plus probable le fait que Lourdes ne soit plus uniquement dédiée au premier type d'actions. De plus, l'engagement significatif de la Russie dans le développement de Cuba pourrait permettre le fonctionnement d'installations de traitement massif de données.

Le fait que la Russie collecte des données sur les câbles depuis Cuba introduirait une rupture importante dans le mode d'action russe, un « expansionnisme ». Cela constituerait un signal fort dans le voisinage immédiat des Etats-Unis, ainsi qu'à destination des pays d'Amérique Latine. La collecte de données « upstream » de la Russie était en effet jusqu'à aujourd'hui centrée sur son propre territoire et son voisinage immédiat, notamment par le biais de SORM.

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

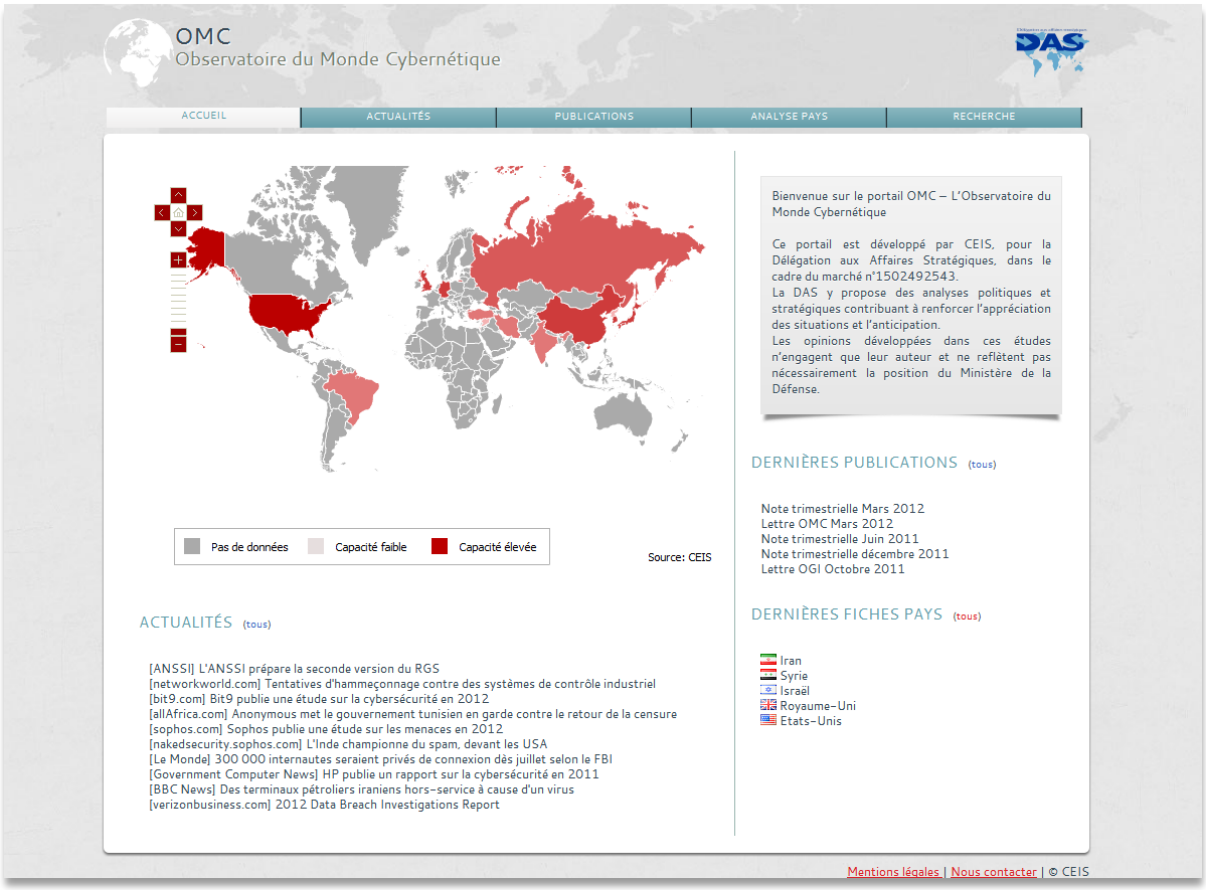


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

AT&T Cyber Security Conference	New York	3 – 4 septembre
du Cyber Security Conference	Dubaï	18 septembre
Chair de Saint - Cyr - Sécurité de l'internet des objets	Paris	19 septembre
Cyber Europe 2014	Belgique	22 - 24 septembre
NFC World Congress	Marseille	22 - 24 septembre
IEEE – Rock Stars of Cybersecurity	Austin	24 septembre
Les Assises de la Sécurité	Monaco	1 - 4 octobre
Cybersecurity in Romania	Sibiu	2 - 3 octobre
Black Hat Briefings & Training Europe	Amsterdam	14 - 17 octobre
X.25 Ethical Hacking Conference	Mexico	17 octobre
Cyber Security SUMMIT 2014	Londres	20 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